



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

5.1.3

JUNE 6, 2025

EFFECTIVE DATE

(06-06-2025)

PURPOSE

- (1) This transmits revised IRM 5.1.3, Safety, Security, and Control.

MATERIAL CHANGES

- (1) The table below contains material changes for this IRM:

IRM Reference	Description of Change
Material Changes section	Updated IRM Material Changes section to comply with January 2025 Executive Orders and OPM guidance.
Throughout IRM	Editorial updates and/or removal of broken links. Editorial update of "Territory Manager" title to "Field Compliance Manager".

EFFECT ON OTHER DOCUMENTS

This material supersedes IRM 5.1.3, dated 08-07-2024.

AUDIENCE

Revenue officers in SB/SE Collection

Thomas Kramer
Director, Collection Policy
Small Business/Self-Employed

5.1.3

Safety, Security, and Control

Table of Contents

5.1.3.1 Program Scope and Objectives

5.1.3.1.1 Background

5.1.3.1.2 Authority

5.1.3.1.3 Roles and Responsibilities

5.1.3.1.4 Program Management and Review

5.1.3.1.5 Program Controls

5.1.3.1.6 Terms and Acronyms

5.1.3.1.7 Related Resources

5.1.3.2 Employee Safety and Security

5.1.3.2.1 Weapons Restriction

5.1.3.2.2 Use of a Pseudonym

5.1.3.2.3 Safety Do's and Don'ts

5.1.3.2.3.1 Safety Issues in the Workplace

5.1.3.2.3.2 Safety Issues in the Field and Office

5.1.3.2.3.3 Minimize Risk of Exposure to Hazardous Substances

5.1.3.2.4 IRS Work-life Program and Services

5.1.3.3 Taxpayer in the Employee Protection System Database

5.1.3.3.1 Office of Employee Protection

5.1.3.3.2 Guidelines for PDT / CAU Coded-Cases

5.1.3.3.2.1 Disclosure Guidelines

5.1.3.3.2.2 PDT Case Procedures

5.1.3.3.2.2.1 Field Contact is Necessary

5.1.3.3.2.2.2 Field Contact is Not Necessary

5.1.3.3.2.3 CAU Case Procedures

5.1.3.3.2.4 PDT / CAU — Referral Procedures

5.1.3.4 Assault, Threat, or Intimidation

5.1.3.4.1 Definition of Terms

5.1.3.4.2 Assault Procedures

5.1.3.4.3 Threat / Intimidation Procedures

5.1.3.4.3.1 Threat of Bodily Harm or Force

5.1.3.4.3.2 Threat of Suicide

5.1.3.4.3.2.1 Suicide Threat Resources

5.1.3.4.3.2.2 Suicide Threat Procedures

5.1.3.4.3.2.2.1 Suicide Threat — Situation 1 — Does Not Require Access to Tax Information

5.1.3.4.3.2.2.2 Suicide Threat — Situation 2 — Requires Access to Tax Information

-
- 5.1.3.4.3.3 Non-Verbal Threats
 - 5.1.3.4.4 Assault / Threat / Intimidation — Reporting Procedures
 - 5.1.3.4.4.1 Preferred Reporting Method to Contact TIGTA
 - 5.1.3.4.4.1.1 Alternate Reporting Method to Contact TIGTA
 - 5.1.3.5 Armed Escort to Contact a Taxpayer
 - 5.1.3.5.1 When to Request Armed Escort
 - 5.1.3.5.2 How to Request Armed Escort
 - 5.1.3.5.2.1 Contacting TIGTA
 - 5.1.3.5.2.2 Contacting CI
 - 5.1.3.5.2.3 Request — One Week Advance Notice/GM Approval
 - 5.1.3.5.2.3.1 Memorandum to TIGTA
 - 5.1.3.5.2.4 Request — Less than One Week Notice
 - 5.1.3.5.3 Armed Escort for a Narcotics Trafficking Case
 - 5.1.3.6 Taxpayer in the Witness Security Program
 - 5.1.3.6.1 Witness Security Program Procedures
 - 5.1.3.6.1.1 Witness Security Coordinator Contact Information
 - 5.1.3.6.1.2 Witness Security Coordinator Procedures
 - 5.1.3.7 Information Security
 - 5.1.3.7.1 Information Gathering Guidelines
 - 5.1.3.7.1.1 Information Gathering Procedures
 - 5.1.3.7.1.1.1 Gathering Information from a Third-Party
 - 5.1.3.7.1.1.2 Notification About Information Gathering
 - 5.1.3.7.2 Personally Identifiable Information
 - 5.1.3.7.2.1 Protecting PII
 - 5.1.3.7.2.1.1 IRS Data Breaches
 - 5.1.3.7.2.1.1.1 Handling Calls from Taxpayers
 - 5.1.3.7.2.1.1.2 Reporting a Potential Privacy or Data Breach
 - 5.1.3.7.3 Property and Records Protection
 - 5.1.3.7.4 Privacy Act
 - 5.1.3.7.4.1 Privacy Act Notification Procedures
 - 5.1.3.7.5 Taxpayer Browsing Protection Act
 - 5.1.3.7.5.1 The UNAX Program
 - 5.1.3.7.5.1.1 UNAX Procedures — Form 11377
 - 5.1.3.8 Internal Control
 - 5.1.3.8.1 Separation of Duties

Exhibits

- 5.1.3-1 Armed Escort Requests- Minimum Required Information

5.1.3.1
(12-15-2020)
Program Scope and Objectives

- (1) **Purpose.** This IRM provides safety, security, and control instructions and guidelines. This IRM covers the following:
 - Employee Safety and Security
 - Taxpayer in the Employee Protection System Database
 - Assault, Threat, or Intimidation
 - Armed Escort to Contact a Taxpayer
 - Taxpayer in the Witness Security Program
 - Information Security
 - Internal Controls
- (2) **Audience.** The procedures are written specifically for revenue officers (ROs). Other employees in Small Business/Self-Employed (SB/SE) and employees in other functions may also refer to these procedures.
- (3) **Policy Owner.** Director, Collection Policy, SB/SE is the policy owner of this IRM.
- (4) **Program Owner.** Collection Policy, SB/SE, Global Strategic Compliance, is the program owner of this IRM.
- (5) **Primary Stakeholders.** The primary stakeholders are SB/SE Collection, SB/SE Operations Support, Office of Employee Protection (OEP), Treasury Inspector General for Tax Administration (TIGTA), and Criminal Investigation (CI).
- (6) **Program Goals.** This guidance contains procedures for employee safety, security and control. Following these procedures will strengthen the public's trust with IRS employees while ensuring the safety of the IRS workforce.

5.1.3.1.1
(08-07-2024)
Background

- (1) The IRS takes security seriously and the safety and welfare of every employee is important. This IRM provides guidance to employees on safety in the workplace and in the field. It also provides guidance on information security.

5.1.3.1.2
(09-23-2019)
Authority

- (1) Congress has delegated to the IRS the responsibility of administering the tax laws, known as the Internal Revenue Code, found in Title 26 of the United States Code. Congress enacts these tax laws, and the IRS enforces them.

5.1.3.1.3
(09-23-2019)
Roles and Responsibilities

- (1) The Director, Collection Policy is the executive responsible for the policy and procedures to be employed by Collection personnel.
- (2) Field Collection Group Managers (GMs) and Field Compliance Managers (FCMs) are responsible for ensuring compliance with the guidance and procedures described in this IRM.

5.1.3.1.4
(08-07-2024)
Program Management and Review

- (1) Program Reports:
 - a. The Collection Activity Reports (CAR) report number 5000-23 provides an overview of staff hours expended and workload data for Field Collection.
 - b. The CAR report number 5000-1 provides an overview of common Taxpayer Delinquent Account (TDA) activity such as issuances, dispositions, credits and inventory.

- c. ENTITY Case Management System receives the Potentially Dangerous Taxpayer (PDT)/Caution Upon Contact (CAU) indicator which is available to query on in inventory and module management. A count of taxpayers with this indicator is also displayed on the ENTITY Open and Queue statistical reports.

(2) Reviews:

- a. Collection Policy conducts program reviews as necessary to verify compliance with IRM requirements and to address TIGTA/General Accounting Office findings.
- b. GMs conduct case reviews to ensure compliance with this IRM.
- c. TM and Area Director conduct operational reviews to evaluate program delivery and conformance to administrative and compliance requirements.

5.1.3.1.5
(08-07-2024)

Program Controls

- (1) GMs, TMs, and area directors are required to approve certain RO case actions. This IRM outlines when approval is required and the level of approval necessary.
- (2) The OEP reviews requests for the input of CAU and PDT indicators and manages those indicators.
- (3) Requests for armed escort must be approved by group managers.
- (4) RO procedures for gathering information are governed by the disclosure provisions, the Privacy Act, third-party contact procedures, and rules about systems of records (SOR).
- (5) Where appropriate, separation of duties is built into RO procedures to act as a deterrent to fraud and concealment.

5.1.3.1.6
(09-23-2019)

Terms and Acronyms

- (1) This table lists commonly used acronyms and their definitions:

Acronym	Definition
BAL DUE	Balance Due
CAR	Collection Activity Reports
CAU	Caution Upon Contact
CI	Criminal Investigation
CSIRC	Computer Security Incident Response Center
DEL RET	Delinquent Return
EAP	Employee Assistance Program
EPS	Employee Protection System
FC	Field Collection
FCM	Field Compliance Manager
FPS	Federal Protective Service

Acronym	Definition
GM	Group Manager
ICS	Integrated Collection System
ID	Identification
IM	Incident Management
IMF	Individual Master File
IT	Information Technology
NFTL	Notice of Federal Tax Lien
OEP	Office of Employee Protection
OI	Other Investigation
PDT	Potentially Dangerous Taxpayer
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information
RO	Revenue Officer
SAC	Special Agent in Charge
SB/SE	Small Business/Self-Employed
SBU	Sensitive But Unclassified
SOR	Systems of Records
TBOR	Taxpayer Bill of Rights
TDA	Taxpayer Delinquent Account
TFRP	Trust Fund Recovery Penalty
TIGTA	Treasury Inspector General for Tax Administration
TIGTA-OI	Treasury Inspector General for Tax Administration, Office of Investigations
USC	United States Code
USMS	United States Marshals Service
WITSEC	Witness Security Program
WSC	Witness Security Coordinator

5.1.3.1.7
(06-06-2025)

Related Resources

- (1) Additional information and guidance can be found in the following IRM sections:
 - IRM 5.1.10.2, Pre-Contact
 - IRM 5.1.22, Disclosure
 - IRM 5.1.28, Identity Theft for Collection Employees
 - IRM 9.2.3.4, Intermediate Weapon Control
 - IRM 10, Security, Privacy and Assurance
 - IRM 11.3, Disclosure of Official Information
 - IRM 25.4, Employee Protection
 - IRM 25.27.1, Third-Party Contact Program
- (2) The IRS adopted the Taxpayer Bill of Rights (TBOR) in June 2014. Employees are responsible for being familiar with and acting in accordance with taxpayer rights. See IRC 7803(a)(3), Execution of Duties in Accord with Taxpayer Rights. For additional information about the TBOR, see *Taxpayer Bill of Rights*.

5.1.3.2
(06-06-2025)

Employee Safety and Security

- (1) Treasury Inspector General for Tax Administration, Office of Investigations' (TIGTA-OI) authority to investigate threats, assaults, and related matters and to conduct armed escorts is derived from the Inspector General Act of 1978 and the Inspector General Reform Act of 2008 and is further described in Treasury Order 115-01. Employees must know what to do to ensure their own personal safety and report threats and assaults. All reports of assaults, threats, or forcible interference against IRS employees performing their official duties must be provided to TIGTA-OI.
- (2) Use common sense to recognize situations which threaten your physical well-being and avoid these situations when possible.
 - a. Avoid subjecting yourself, the taxpayer, or any third-party to a potentially dangerous situation.
 - b. Be aware of potential safety and health risks when entering premises where there is a possible risk of exposure to hazardous substances.
- (3) The Field Employees Credential (ID) Verification Program provides local law enforcement and taxpayers the means to verify an IRS field representative is a current employee of the IRS. For additional information, see the Field Employees Credential (ID) Verification Program section on the Employee Resources, Physical Security, IRS Identification Cards SharePoint page. Document 13345, IRS Field Employee Verification Phone Numbers, is an internal use card carried by IRS Field employees for use when their identity is challenged. See IRM 5.1.10.3, Initial Contact, for additional information.

5.1.3.2.1
(09-23-2019)

Weapons Restriction

- (1) An RO is prohibited from carrying a weapon. Even though the RO position involves some potential for risk when contacting a taxpayer (or a third-party), an RO is not authorized to carry and/or use a firearm(s) in the performance of official duties. This restriction includes pepper spray, "Halt!" Dog Repellent, or any other "intermediate" weapon. IRM 9.2.3.4, Intermediate Weapon Control, defines intermediate weapons as weapons other than firearms or lethal weapons with non-lethal munitions, designed to supplement weaponless control techniques.
- (2) Any time you think it will be necessary to ensure your safety, request (through your manager) that an armed escort from TIGTA be assigned to accompany

you when contacting a taxpayer in person. See IRM 5.1.3.5, Armed Escort to Contact A Taxpayer.

5.1.3.2.2
(09-23-2019)
Use of a Pseudonym

- (1) An RO may be authorized to use a pseudonym if they can provide adequate justification for using a pseudonym. An RO is not entitled to use a pseudonym without adequate justification. Additionally, the GM must approve the RO's use of a pseudonym. Adequate justification includes "protection of personal safety."
- (2) Refer to IRM 10.5.7, Use of Pseudonyms by IRS Employees, for further information.

5.1.3.2.3
(08-07-2024)
Safety Do's and Don'ts

- (1) Follow the guidance displayed in the tables below:

Safety Do's

Do:
Research the case prior to contacting the taxpayer or third parties.
Prepare interview questions in advance.
Rehearse how you would react to a situation and have a backup plan.
Bring another RO to accompany you, if necessary.
Arrange for an armed escort, if necessary.
Secure maps of assigned area.
Dress appropriately for the environment.
Store valuables in the trunk of your car.
Observe your surroundings, including exits and others who are present.
Be alert for "No Trespassing" or warning signs.
Park your vehicle so you can leave quickly.
Maintain at least an arm's length distance from the taxpayer.
Stay alert.
Act professionally.
Stay in control of the interview.
Inform your manager or a co-worker of your location and status before and after taxpayer contact, if necessary.

Safety Don'ts

Do Not:
Repeatedly call the taxpayer for additional information.
Lose focus.

Do Not:
Personalize collection efforts.
Threaten or patronize the taxpayer.
Be overzealous.
Try to be funny or witty.
Use a threatening tone of voice or body language.
Mislead the taxpayer.
Be afraid to seek assistance.
Lose composure.
Turn your back on the taxpayer.
Enter areas with unleashed animals.
Try to prevent rescue of seized property.

5.1.3.2.3.1
(08-07-2024)

Safety Issues in the Workplace

- (1) Follow this guidance to ensure your safety in the workplace:
 - a. Wear your identification (ID) badge.
 - b. Safeguard your keys, key card, ID badge, and any combinations to work locks and promptly report the theft or loss of any of these items.
 - c. Consider using the “buddy system” when leaving the workplace, especially after dark, and either leave in a group of people or have someone watch you from inside the building as you walk to your car.
 - d. Be vigilant at all times.
 - e. Be familiar with your surroundings.
 - f. Notice when something is not right and report it to your manager or local authority.
- (2) Do not ignore it if something seems “out of the ordinary”.
 - a. Tell your supervisor when you notice anything suspicious, such as an emergency exit or window left open.
 - b. Challenge any unidentified individuals you encounter in the workplace who is not wearing an ID badge.

Example: An RO sees a stranger in the office area and the person is not wearing a visible ID badge. The RO should ask to see the person’s ID badge. If the RO is not comfortable confronting the person directly, they should report the person to their manager or another nearby supervisor.

- (3) In office appointments:
 - a. Greet and escort the taxpayer into and out of your meeting space.
 - b. When possible, utilize interview rooms with operable duress buttons.
 - c. Consider partnering with another in-office revenue officer.
 - d. If the taxpayer becomes highly agitated, terminate the interview and escort the taxpayer out of the office. If necessary, solicit assistance from

another employee, building security officer, TIGTA, or local authorities. See IRM 10.2.8, Physical Security Program - Incident Reporting, for additional reporting requirements.

- e. See IRM 5.1.3.4, Assault, Threat, or Intimidation.

5.1.3.2.3.2 (08-07-2024) Safety Issues in the Field and Office

- (1) The public's trust in the IRS has been affected by various external factors such as the rise of IRS impersonation scams, identity theft and cyber security threats. Scams have taken many shapes and forms, such as phone calls, letters and emails. Many IRS impersonators use threats to intimidate and bully people into paying a fabricated tax bill. They may even threaten to arrest or deport their would-be victim if the victim does not comply. The IRS communicates with taxpayers to help keep them safe from the various scams and IRS impersonation schemes that could affect them. These fraudulent activities can also affect Field employees. Revenue officers may face additional scrutiny or safety concerns due to taxpayer suspicion that the RO is not a legitimate IRS employee. To promote public trust, properly identify yourself as an employee of the IRS when interacting with taxpayers and third parties associated with your collection case, and do not misrepresent yourself or your reason for contact with the public. Refer to IRM 5.1.10.3, Initial Contact, and IRM 5.1.10.6.4, Promoting Public Confidence, for additional details and situations where exceptions may apply.
- (2) Follow this guidance to help ensure your safety in the field and in the office:
 - a. Be vigilant at all times.
 - b. Notice when something is not right and consider reporting it to a local authority.
 - c. See IRM 10.2.8, Incident Reporting, for additional reporting requirements.
- (3) If you encounter "No Trespassing" signs, follow guidance in IRM 5.1.10.6.2, No Trespassing Signs.
- (4) See IRM 5.1.10.2, Pre-Contact, for steps to take when planning field visits to minimize the risk.
- (5) Follow the guidance displayed in the table below:

Safety Issues in the Field and Office

If...	And...	Then...
The taxpayer appears highly agitated during a scheduled appointment at their premises	does not want you to enter the premises,	<ul style="list-style-type: none">• Try to schedule an office appointment, or• Suggest that the taxpayer assign a power of attorney to handle the matter.
There is/are a third-party(ies) present at a scheduled appointment	they are contributing to an increasingly hostile environment,	<ul style="list-style-type: none">• Terminate the interview and exit the premises.• If in the office, solicit the assistance of another employee or building security to escort the third party from the premises.

If...	And...	Then...
The taxpayer has an intimidating animal	the interview is not going well in the field or the office,	<ul style="list-style-type: none"> Ask the taxpayer to remove the animal, or Conclude the interview as quickly as possible, or Terminate the interview and leave, if necessary.
There is a weapon near the taxpayer	you are in the field,	<ul style="list-style-type: none"> Terminate the interview and leave. Follow-up with a telephone call, or Ask the taxpayer to come into the office. <p>Note: It is not unlawful for an individual to own a firearm unless the individual is exempt from ownership by law under 18 USC 922 (g) and (n). If there is a firearm and the individual is exempt from ownership, contact your local TIGTA office.</p>
The taxpayer has a weapon, or you suspect the taxpayer has a weapon in their possession	you are in the office,	<ul style="list-style-type: none"> If the office has on-site security staffing, notify the security guard and request guidance. Notify your immediate supervisor, or another authorized management official if your manager is not available and request guidance. See IRM 10.2.8.2, Incident Reporting, for additional reporting requirements.

5.1.3.2.3.3
(09-23-2019)

**Minimize Risk of
Exposure to Hazardous
Substances**

(1) The nature of a business can be an indicator that further investigation is required before entering the premises. Federal, state and some local regulations require business owners to maintain a list of all hazardous chemicals in the workplace on a material safety data sheet.

(2) The following are examples of a certain type of business which might require extreme caution:

- a. Chemical storage company
- b. Asbestos abatement company
- c. Environmental mitigation company

Note: This list is not all-inclusive.

(3) Follow this guidance to ensure your safety in the field:

- a. Use extreme caution when you cannot determine the potential risk before a field call or if the potential risk does not become known until after entering the premises.
- b. Consider contacting the Environmental Protection Agency or appropriate state agency for assistance if it is suspected that the taxpayer sells or maintains industrial or commercial chemicals.
- c. Request the taxpayer to provide a copy of the material safety data sheet before making a field call or at the start of a field call.

5.1.3.2.4
(06-06-2025)
**IRS Work-life Program
and Services**

- (1) IRS Work-life Programs and Services help you balance your job at the IRS with your life outside of work.

5.1.3.3
(09-23-2019)
**Taxpayer in the
Employee Protection
System Database**

- (1) The IRS has developed the Employee Protection System (EPS) to protect IRS public contact employees. There are two Servicewide employee safety programs under the EPS:
 1. The PDT Program that identifies taxpayers who represent a potential danger to IRS public contact employees
 2. The CAU Taxpayer Program that identifies a taxpayer who should be approached with caution

5.1.3.3.1
(06-06-2025)
**Office of Employee
Protection**

- (1) OEP has sole responsibility for administering the two Servicewide employee safety programs. OEP enhances the safety of IRS public contact employees by:
 - maintaining IRM 25.4, Employee Protection
 - maintaining the OEP web site
 - maintaining the PDT and CAU indicators on IDRS
- (2) OEP maintains two IRMs that provide guidance and information:
 - a. IRM 25.4.1, Potentially Dangerous Taxpayer, provides procedures and guidelines for referring and designating taxpayers under the PDT program. Exhibit 25.4.1-1, Display of “PDT” Indicator, provides a list of documents that display the PDT indicator.
 - b. IRM 25.4.2, Caution Upon Contact Taxpayer, provides procedures and guidelines for referring and designating taxpayers under the CAU Taxpayer program. Exhibit 25.4.2-1, Display of CAU Indicator, provides a list of documents that display the CAU indicator.
- (3) OEP maintains a Knowledge Management resource library under Data and Employee Protection on the Disclosure and Privacy Knowledge Base.
- (4) Any of the following types of cases may be coded PDT or CAU:
 - Balance Due (BAL DUE) Account
 - Delinquent Return (DEL RET) Account
 - Other Investigation (OI), etc.

5.1.3.3.2
(09-23-2019)
**Guidelines for PDT /
CAU Coded-Cases**

- (1) Field Collection (FC) employees must become aware of the IRM procedures and IRS Source guidelines for dealing with PDT-coded cases and CAU-coded cases. As needed, FC employees should:
 - a. review the OEP IRMs.
 - b. access the OEP web site.
 - c. feel free to contact OEP to discuss a taxpayer’s case to resolve any PDT or CAU questions.

- (2) Be alert for PDT-coded cases and/or CAU-coded cases in your case inventory.

Note: See IRM 25.4.1.7, Power of Attorney (POA) Information, and/or IRM 25.4.2.6, Power of Attorney (POA) Information, for guidance about utilizing IDRS to ascertain whether a POA has been designated as PDT or CAU.

	(3) Review each case (Integrated Collection System (ICS) screens, IDRS printouts, etc.) for a PDT or CAU designation.
5.1.3.3.2.1 (06-01-2010) Disclosure Guidelines	<p>(1) Occasionally, a taxpayer will question if the IRS has placed a PDT or CAU designation on their tax account.</p> <p>(2) Take the following action if a taxpayer makes an inquiry about their PDT / CAU designation status:</p> <ol style="list-style-type: none"> Do not confirm or deny that their case is coded PDT or CAU. Forward the taxpayer's request to Disclosure. <p>Note: Disclosure will respond to the taxpayer's inquiry.</p>
5.1.3.3.2.2 (09-23-2019) PDT Case Procedures	<p>(1) TIGTA is responsible for providing an armed escort when a taxpayer is coded as a PDT. The request for an armed escort will be made via memorandum from the employee's supervisor to the TIGTA Special Agent in Charge (SAC) of the division where the escort is needed. See IRM 5.1.3.5, Armed Escort to Contact a Taxpayer. The RO should not schedule a taxpayer appointment until the supervisor has spoken to the TIGTA special agent assigned to the armed escort.</p> <p>(2) Consider alternatives to contacting a taxpayer in the field when:</p> <ul style="list-style-type: none"> the case is designated a PDT, or a "potentially dangerous" designation is under investigation. <p>(3) Avoid in-person contact, if possible, when a taxpayer's case is coded a PDT.</p> <p>(4) Determine if field contact is necessary to handle the case and follow the appropriate procedures below:</p> <ol style="list-style-type: none"> IRM 5.1.3.3.2.2.1, Field Contact is Necessary. IRM 5.1.3.3.2.2.2, Field Contact is Not Necessary.
5.1.3.3.2.2.1 (06-01-2010) Field Contact is Necessary	<p>(1) Consider armed escort in all PDT-coded cases.</p> <p>(2) Notify TIGTA for advice when you anticipate making a field call on a PDT-coded case.</p> <p>(3) Follow TIGTA's advice when you make field contact on a PDT-coded case.</p> <p>(4) Take appropriate collection action.</p>
5.1.3.3.2.2.2 (06-01-2010) Field Contact is Not Necessary	<p>(1) Avoid in-person contact with the taxpayer coded PDT.</p> <p>(2) Take appropriate collection action over the phone and/or through the mail.</p>
5.1.3.3.2.3 (09-23-2019) CAU Case Procedures	<p>(1) Approach a taxpayer coded CAU with caution.</p> <p>(2) Consider armed escorts in a CAU-coded cases. See IRM 5.1.3.5, Armed Escort to Contact a Taxpayer.</p>

5.1.3.3.2.4
(08-07-2024)
PDT / CAU — Referral Procedures

- (3) Take appropriate collection action in-person and/or over the phone and/or through the mail.
- (1) Occasionally, an IRS public contact employee might question if a taxpayer's tax account should be designated PDT or CAU.
- (2) Take some or all of the following actions when you believe you should refer a taxpayer for a PDT or CAU indicator:
 - a. Access the OEP web site.
 - b. Consult with OEP. See IRM 25.4.1.3, Reporting to TIGTA, if you believe a taxpayer's account should be coded PDT. See IRM 25.4.2.2, The CAU Program, if you believe a taxpayer's account should be coded CAU.
- (3) Make a referral for an appropriate PDT or CAU when you believe it is necessary.

5.1.3.4
(09-23-2019)
Assault, Threat, or Intimidation

- (1) While the overwhelming majority of Americans respect IRS employees and the IRS mission, employee safety is critical. The actual number of threats and assaults is low given the number of contacts that we make in a given year. While the majority of us go through our careers without incident, one incident would be too many when it comes to employee safety. Unfortunately, a taxpayer (or a third-party) experiencing financial difficulties, such as multiple financial debts, may feel increased pressure and act out aggressively. Occasionally, a taxpayer (or a third-party) will assault, threaten, or intimidate an IRS public contact employee; and/or a taxpayer might make an assault upon an IRS employee.
- (2) TIGTA handles threats of suicide by a taxpayer as well as taxpayer threats against IRS personnel. TIGTA takes its responsibility to protect IRS employees extremely seriously. TIGTA will:
 - Take swift action and will maintain continuous, open communication during a case.
 - Make a decision regarding any necessary protective measures, including initiating PDT cases. See IRM 25.4.1.1.2.2, TIGTA's Role.
- (3) As an IRS public contact employee, you must:
 - a. Remain alert to act quickly in a dangerous situation.
 - b. Continue to be aware of your surroundings when knocking on the door of a taxpayer or third-party and when entering a taxpayer's premises.
 - c. Trust and rely on your instincts.
 - d. Report incidents of assault, threat, intimidation, or forcible interference to TIGTA.
- (4) The IRS Work-life Program and Services is available to help IRS employees and their families overcome stressful life issues and personal concerns. See IRM 5.1.3.2.4, IRS Work-life Program and Services.

5.1.3.4.1
(06-01-2010)
Definition of Terms

- (1) Three terms are applicable to this discussion: assault, threat, and intimidate. These terms are defined below, but these definitions are not intended as the legal definitions of the terms; they are provided to clarify the terms.

- 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 an action.

5.1.3.4.2
(09-23-2019)

Assault Procedures

- (1) With any type of assault situation, the safety of our workforce is paramount and our first concern.
- (2) Continue to be vigilant and remain alert in your surroundings. A taxpayer may make a threat to express anger or try to intimidate you to impede your duties.
- (3) Take the following action immediately if you are assaulted while performing official duties during a personal interview or in connection with the performance of official duties:
 - a. Defend or protect yourself from further assault.
 - b. Terminate collection activities.
 - c. Leave the site of the incident, if safe to do so.
 - d. If the threat is imminent, call 911.
 - e. Obtain medical treatment, if necessary.
- (4) The employee should make every attempt to document the incident, to include location, individuals involved, actions taken, statements made, the involvement of weapons, the presence and nature of signs posted on the property/location, etc.
- (5) Report the incident to TIGTA as soon as possible.

5.1.3.4.3
(09-23-2019)

**Threat / Intimidation
Procedures**

- (1) With any type of threat situation, the safety of the workforce is of paramount concern. A taxpayer may make a verbal threat of harm, force, or suicide either during a personal interview or a telephone conversation to express anger, emotion, or try to intimidate you to impede your duties.

Reminder: TIGTA handles threats of suicide by a taxpayer as well as taxpayer threats against IRS personnel; contact TIGTA if you receive a suicide threat.

- (2) Continue to be vigilant and remain alert in your surroundings.
- (3) Always take the threat seriously and act quickly.
- (4) Take the following applicable action, depending upon the situation:
 - a. IRM 5.1.3.4.3.1, Threat of Bodily Harm or Force.
 - b. IRM 5.1.3.4.3.2, Threat of Suicide.

5.1.3.4.3.1
(09-23-2019)

Threat of Bodily Harm or Force

- (1) Take the following action if you receive a verbal (or other) threat of bodily harm or force:
 - a. Leave the taxpayer's premises immediately if threatened or assaulted.
 - b. Do not let a confrontation escalate.
 - c. Do not induce perpetrators to clarify or repeat threatening statements.
 - d. Avoid questions such as "Is that a threat?" or "Are you threatening me?"
 - e. Tactfully end the conversation, if possible.
 - f. Document as much detail about the threat as possible, e.g., date, time, place, type, and exactly what, to your best memory, the taxpayer said and did.
- (2) Report the incident to TIGTA as soon as possible. See IRM 5.1.3.4.4.1, Preferred Reporting Method to Contact TIGTA.
- (3) Do not make further contact with the taxpayer until:
 - a. You have referred the threat to TIGTA, and
 - b. TIGTA has made a decision and notified you regarding protective measures.

5.1.3.4.3.2
(09-23-2019)

Threat of Suicide

- (1) Pre-reading the suicide threat guidance may prepare you to take a suicide threat seriously and to act quickly when a suicide threat occurs.
- (2) Always take a suicide threat seriously and act quickly if you encounter a taxpayer who threatens suicide.
- (3) Follow the procedures below if you receive a suicide threat:
 - IRM 5.1.3.4.3.2.1, Suicide Threat Resources
 - IRM 5.1.3.4.3.2.2, Suicide Threat Procedures

5.1.3.4.3.2.1
(06-06-2025)

Suicide Threat Resources

- (1) Refer to IRM 11.3.28.7.1, Suicide Threats, for information about handling a suicide threat.
- (2) See IRM 5.1.3.4.3.2.2, Suicide Threat Procedures.

5.1.3.4.3.2.2
(06-06-2025)

Suicide Threat Procedures

- (1) Employees must become familiar with the procedures for dealing with a suicide threat in order to take quick action and provide the correct response when a suicide threat happens.

Reminder: TIGTA handles threats of suicide by a taxpayer as well as taxpayer threats against IRS personnel.

- (2) Take the following action if you receive a suicide threat:
 - a. Take the threat seriously regardless of whether you think it may be serious or not, as you have no way to make that determination.
 - b. Act quickly. Be ready and willing to get help. Consider getting another employee's attention as soon as you receive the threat. Eliciting assistance from an employee(s) around you may help you take the appropriate action.
 - c. Stay calm and remain with the individual, whether in-person or on the phone. A calm demeanor and a caring voice may help to defuse the situation.

- d. Determine the information you need to notify the authorities who can help the individual.
- (3) Take the following action to obtain the necessary information if you are not with the individual:
 - a. Ask the individual for their address or location.
 - b. Check public sources of address information; look in the telephone book, Internet, or other public sources.
- (4) See IRM 25.4.2.3, CAU Determination and Appeal, for information on completing and submitting Form 13090, Caution Indicator Referral Report, to the OEP when a taxpayer threatens suicide.
- (5) Take the following applicable action depending upon the situation:
 - IRM 5.1.3.4.3.2.2.1, Suicide Threat - Situation 1 - Does Not Require Access to Tax Information.
 - IRM 5.1.3.4.3.2.2.2, Suicide Threat - Situation 2 - Requires Access to Tax Information.

5.1.3.4.3.2.2.1
(08-07-2024)

**Suicide Threat —
Situation 1 — Does Not
Require Access to Tax
Information**

- (1) Situation 1 applies when you are with the individual or the individual's location comes from the individual or a public source and does **not** require you to access tax information. By itself, a threat of suicide is not considered tax information and is not covered by the rules limiting tax disclosures.
 - a. Immediately call 911 for assistance, if available. Otherwise contact the appropriate state or federal law enforcement authorities.
 - b. Report that an individual has threatened suicide.
- Caution:** Only disclose the information necessary to help 911 (or other law enforcement authorities) to locate the individual. State that the threat was made during a contact involving "official business." Do not mention the underlying reason for the contact or that it is related to a tax issue.
- c. Provide the name and location of the individual.
 - d. Contact TIGTA or ask your GM or a co-worker to notify TIGTA as soon as possible. See IRM 5.1.3.4.4.1, Preferred Method to Contact TIGTA.

5.1.3.4.3.2.2.2
(08-07-2024)

**Suicide Threat —
Situation 2 — Requires
Access to Tax
Information**

- (1) Situation 2 applies when you cannot obtain the individual's location from a public source requiring you to access tax information (e.g., check IDRS) to obtain the individual's address. The procedures for a disclosure under IRC 6103(i)(3)(B)(i) apply when the possibility of death or physical injury exists. Delegation Order 11-2, Authority to Permit Disclosure of Tax Information and to Permit Testimony or the Production of Documents, provides delegated authority to an IRS supervisory employee or CI special agent to make disclosure to state or federal law enforcement authorities.
 - (2) Check IDRS or other tax sources, for example: a copy of the individual's tax return or other document in the case file, to ascertain the individual's address.
- Caution:** An RO is not authorized to make the disclosure.
- (3) Do not make the disclosure yourself; instead, follow these procedures:

- a. Contact your GM. If your GM is not available, contact another authorized supervisory level employee (for example: another GM, a manager in your local Disclosure Office, etc.) to make the disclosure, or contact a CI special agent.
- b. Apprise your GM, the IRS supervisory level employee, or CI special agent, as applicable, of the suicide threat and provide them with the individual's address.

Note: The authorized employee must follow the procedures displayed in the following table.

Procedures for an Authorized Employee to Report the Suicide Threat	
1.	Immediately call 911 for assistance, if available. Otherwise contact the appropriate state or federal law enforcement authorities.
2.	Report that an individual has threatened suicide.
3.	Provide the name and location of the individual. Caution: Only disclose the information necessary to help law enforcement authorities locate the individual. State that the threat was made during a contact involving "official business." Do not mention the underlying reason for the contact or that it is related to a tax issue.
4.	Contact TIGTA as soon as possible.
5.	See IRM 5.1.3.4.4.1, Preferred Reporting Method to Contact TIGTA.
6.	Report the disclosure to the local Disclosure Office for accounting purposes after you make the disclosure.
7.	See IRM 11.3.28.7.1, Suicide Threats.

5.1.3.4.3.3
(08-07-2024)
Non-Verbal Threats

- (1) A non-verbal threat has the same purpose as a verbal threat, that is, to intimidate or impede your duties. Non-verbal threats include gestures, motions, or a display of weapons. A non-verbal threat may also be made in a document, such as, disturbing pictures or illustrations.
 - a. Treat a non-verbal threat with the same caution as a verbal threat.
 - b. Follow the same pattern of avoidance as directed above. See IRM 5.1.3.4.3.1, Threats of Bodily Harm or Force.
 - c. Retreat from continued contact if you receive a non-verbal threat.
 - d. Report the incident to TIGTA as soon as possible. See IRM 5.1.3.4.4.1, Preferred Reporting Method to Contact TIGTA.

5.1.3.4.4
(06-06-2025)
Assault / Threat / Intimidation — Reporting Procedures

- (1) Report assaults or threats as soon as possible to your GM and TIGTA. See IRM 5.1.3.4.4.1, Preferred Reporting Method to Contact TIGTA.
- (2) Consider contacting EAP to seek assistance to overcome any stress caused by an assault or threat. See IRM 5.1.3.2.4, IRS Work-Life Program and Services.

Note: GMs should consider contacting EAP to arrange for critical / traumatic incident services when a critical / traumatic incident involves or directly impacts the workplace.

5.1.3.4.4.1
(06-06-2025)

**Preferred Reporting
Method to Contact
TIGTA**

- (1) The preferred method to make a report to TIGTA is by one of the following methods:
 - a. Contact your local TIGTA point of contact. If you cannot reach your local TIGTA point of contact, call 800-589-3718 to report threats, bribes, or computer intrusions. This phone number reaches a contracted company that answers calls on behalf of TIGTA 24 hours a day 7 days a week but **only** for exigent issues such as threats, bribes, or computer intrusions when the local TIGTA point of contact cannot be reached.
 - b. Online via *Submit a Complaint*.
 - c. Phone: call the TIGTA National Hotline at 1-800-366-4484.

5.1.3.4.4.1.1
(06-06-2025)

**Alternate Reporting
Method to Contact
TIGTA**

- (1) Reporting by mail is an alternate reporting method:
 Treasury Inspector General for Tax Administration
 Hotline Team
 P.O. Box 23291
 Washington, DC 20026
- (2) Locate additional contact information for TIGTA at *U.S. Treasury Inspector General For Tax Administration* and click on "Report Waste, Fraud, and Abuse".

5.1.3.5
(09-23-2019)

**Armed Escort to Contact
a Taxpayer**

- (1) IRS public contact employees may require protection if threatened with bodily harm by a taxpayer or if other circumstances develop which interfere with the administration of Internal Revenue laws. On April 26, 2011, TIGTA-OI issued a memorandum entitled "Armed Escort Program" to provide notification about changes to armed escort procedures. Effective May 2, 2011, TIGTA-OI assumed responsibility for all armed escorts; however, IRS-CI will continue to provide protection for the Commissioner of Internal Revenue. Prior to this change, TIGTA-OI and IRS-CI shared responsibility for providing armed escorts. Unless specifically asked for assistance by TIGTA-OI, IRS-CI will no longer be responsible for providing armed escorts to IRS employees. If IRS-CI assistance is needed, TIGTA-OI will coordinate with their local IRS-CI office regarding the armed escort.
- (2) Follow these procedures when you need to arrange an armed escort.

5.1.3.5.1
(09-23-2019)

**When to Request Armed
Escort**

- (1) Armed escorts may be requested in circumstances where the employee and their manager believe interaction with a taxpayer or third-party may pose a risk of injury to the employee. Review IDRS to determine if PDT or CAU coding has been added to the taxpayer's account. Request armed escort to accompany you on any case (that is, BAL DUE, DEL RET, OI, etc.) to contact a taxpayer, either for an in-office interview or a field call, when you believe armed escort is necessary because the taxpayer or third-party:
 - a. intends to interfere with collection activity.
 - b. uses or threatens to use force.

- c. is the subject of an open TIGTA assault or threat investigation.
 - d. has a PDT indicator on their account.
- (2) You may encounter interference with collection activity when you seize property. You may also encounter the use of force or a threat of force during any other face-to-face interview or meeting. Consider requesting armed escort when you believe a taxpayer or third-party intends to interfere with collection activity.
 - (3) Always request armed escort when a person (or persons) uses force or threatens to use force or if the case is coded PDT.
 - (4) Prior to submitting a request for armed escort in a case coded CAU, contact OEP to ascertain the basis for the CAU designation. Your manager must evaluate this information to determine if an armed escort is justified.
 - (5) Consider asking the taxpayer to meet you at your office even if you believe an armed escort is not required. Sometimes the best place to talk to a taxpayer is in an IRS office. Bringing a person out of their comfort zone may diffuse tension that would lead to a threat.
 - (6) Consider asking TIGTA to have a special agent available when you meet with a taxpayer in your office. Depending on the circumstance, TIGTA may provide a special agent to sit-in on an in-office interview with you, or to be close by during the interview, in case of any trouble. Sometimes, just knowing a Special Agent is nearby can be comforting and helpful for you to get your job done effectively and efficiently. Your manager will coordinate these requests through the nearest TIGTA-OI office.
 - (7) As warranted, TIGTA-OI may provide armed escorts to IRS personnel, IRS contractors, informants, witnesses, and other eligible persons.

5.1.3.5.2
(08-07-2024)
How to Request Armed Escort

- (1) Revenue officers prepare an encrypted email request and send it to their group manager for review. Group managers submit the request via memorandum to the TIGTA-OI SAC of the division where the escort is needed. See IRM 5.1.3.5.2.1, Contacting TIGTA.
- (2) The email may have an attached memorandum with all required facts or simply include a statement of all required facts within the body of the email. When preparing a memorandum, follow the format shown in IRM 5.1.3.5.2.3.1, Memorandum to TIGTA.
- (3) Include all pertinent facts and circumstances in the request. The request must include the *minimum information* shown in Exhibit 5.1.3-1, Armed Escort Requests-Minimum Required Information.
 - a. State the nature of the investigation (that is, balance due account, delinquent return, periods, type of tax, amounts due, etc.).
 - b. State why an armed escort is necessary. Include the following information: What did the taxpayer do or say to indicate potential trouble; knowledge of any weapons the taxpayer may have; were any actions taken, or anything said that upset the taxpayer; are there potential hazards in the area; what do you want to achieve.
- (4) Requests must be submitted to TIGTA-OI *at least* one week prior to the date the escort is needed.

- (5) If a request is submitted to TIGTA-OI with less than one week's notification, postponement of the meeting or change to an alternate location may be required.
- (6) The respective TIGTA-OI SAC will review all armed escort requests for approval on a case-by-case basis. If the TIGTA-OI SAC determines that an armed escort is not warranted, IRS management may seek *reconsideration* of the denied request by contacting the TIGTA-OI SAC who rendered the decision. In the event the SAC's decision remains unchanged, and the re-requesting IRS management official still believes an armed escort is warranted, they can request a *final reconsideration* from the SAC's immediate executive.

5.1.3.5.2.1
(06-06-2025)
Contacting TIGTA

- (1) Managers contact the appropriate TIGTA-OI SAC via **secure** email containing a memorandum to request armed escort when they agree that the request is justified. See IRM 5.1.3.5.2.3, Request-One Week Advance Notice/GM Approval.
- (2) Contact your local TIGTA Special Agent to determine whom the armed escort memorandum should be addressed. The following link can be used to identify the location of the closest TIGTA office: *Office of Investigations Divisions*.

5.1.3.5.2.2
(09-23-2019)
Contacting CI

- (1) As TIGTA-OI has sole authority and responsibility for providing armed escorts, IRS employees/managers may NOT request and/or alternately seek assistance from IRS-CI if the request for armed escort is denied. See IRM 5.1.3.5.2, How to Request Armed Escort, for TIGTA-OI appeal procedures.
- (2) If IRS-CI receives a request for armed escort from an IRS employee/manager, CI will refer them to the nearest TIGTA-OI office.
- (3) If TIGTA-OI determines that IRS-CI assistance is needed, they will coordinate with their local IRS-CI office regarding the armed escort.

5.1.3.5.2.3
(09-23-2019)
Request — One Week Advance Notice/GM Approval

- (1) Generally, the TIGTA-OI SAC must receive the request for armed escort at least one week prior to the date the armed escort is needed. One week advance notice is required in order to ensure the safety of IRS and TIGTA-OI personnel as well as reduce operational risk of the armed escort.
- (2) Follow these steps to obtain *managerial approval* for armed escorts:
 - 1. Prepare an email message that includes all necessary information. See IRM 5.1.3.5.2, How to Request Armed Escort.
 - 2. If you prepared a memorandum, add the document as an attachment to the email. Memorandums should not exceed two pages.
 - 3. Send the request to your GM via encrypted email.

Note: Management must follow the established procedures (displayed in the following table) to arrange armed escort.

Managerial Procedures for Arranging Armed Escort
<p>The GM must do the following after receipt of the armed escort request from the RO:</p> <ol style="list-style-type: none"> Decide if an armed escort is justified. See IRM 5.1.3.5.1, When to Request Armed Escort. Ensure that all pertinent facts and circumstances are included in the request. See Exhibit 5.1.3-1, Armed Escort Requests- Minimum Required Information, for the minimum information that <i>must</i> be provided. Prior to submitting a request for cases with the CAU indicator, the employee or manager must contact the OEP to ascertain the basis for OEP's CAU designation. Managers must evaluate this information and proceed with the armed escort request only if they agree that an armed escort is still necessary. Forward the request for armed escort to the appropriate TIGTA-OI SAC via secure email. See IRM 5.1.3.5.2.1, Contacting TIGTA.

5.1.3.5.2.3.1
(06-06-2025)
Memorandum to TIGTA

- (1) Follow this format to prepare the memorandum to TIGTA:
 - To:** Treasury Inspector General for Tax Administration, Attn: Special Agent in Charge, ____ [Field Division] (Include the division name (e.g., Southern Field Division, Northeastern Field Division, Western Field Division, etc.) Field divisions are identified on the TIGTA website at: *Office of Investigations Divisions*.)
 - From:** _____, Group Manager
 - Subject:** Request for Armed Escort to Accompany Revenue Officer _____
- (2) Include all pertinent information as explained in IRM 5.1.3.5.2, How to Request Armed Escort.
- (3) Memorandums should not exceed two pages in length.

5.1.3.5.2.4
(02-23-2012)
Request — Less than One Week Notice

- (1) If TIGTA-OI does not receive the request at least one week prior to the date the armed escort is needed you may have to reschedule the planned visit and/or change the location of the meeting.

5.1.3.5.3
(09-23-2019)
Armed Escort for a Narcotics Trafficking Case

- (1) A narcotics trafficking case is any case (that is, BAL DUE, DEL RET, OI, etc.) involving an individual connected with narcotics trafficking.
 - Generally, an armed escort is required to personally contact the subject of a narcotic trafficker assessment or investigation.
 - However, when certain conditions apply, armed escort is not required.
- (2) Arrange for armed escort to contact a taxpayer unless one of the following conditions exists:
 - The trafficker is in protective custody, or
 - Information is available which clearly establishes that personal contact would not place the employee at risk of physical harm (e.g., numerous prior contacts have been made without incident.)

- (3) Follow the above procedures if you need to request armed escort. See IRM 5.1.3.5, Armed Escort to Contact a Taxpayer.

5.1.3.6
(09-23-2019)
**Taxpayer in the Witness
Security Program**

- (1) The Witness Security Program (WITSEC) was authorized by the Organized Crime Control Act of 1970 and amended by the Comprehensive Crime Control Act of 1984. WITSEC is a witness protection program administered by the United States Department of Justice and operated by the United States Marshal Service (USMS). The successful operation of this program is widely recognized as providing a unique and valuable tool in the government's war against major criminal conspirators and organized crime.
- (2) Under WITSEC, the USMS provides for the security of government witnesses and their families, whose lives are in danger as a result of their testimony against drug traffickers, terrorists, organized crime members and other major criminals. Witnesses and their families in the program have been protected, relocated, and given new identities by the USMS.

5.1.3.6.1
(06-06-2025)
**Witness Security
Program Procedures**

- (1) A person in WITSEC will not disclose they are in this program. The RO should not make inquiries of the taxpayer or the USMS asking if the person is in WITSEC.
- (2) Generally, when Collection contacts a witness in WITSEC, the witness will notify the USMS, who will contact the SB/SE Witness Security Coordinator (WSC). The WSC will contact the proper management chain of the RO with instructions.
- (3) If an RO suspects, or becomes aware, that a taxpayer is in WITSEC, they should:
 - a. Cease all efforts to locate the taxpayer immediately.
 - b. Cease all collection activity. Do not make a Notice of Federal Tax Lien (NFTL) determination. Do not file a NFTL.
 - c. Notify the WSC by preparing a memorandum to advise your GM and the TM that the taxpayer may be in the WITSEC.
- (4) Follow this format to prepare the memorandum:
 - To: (Field Compliance Manager's Name), Field Compliance Manager
 - Through: (Manager's Name), Group Manager
 - From: (Your Name), Revenue Officer
 - Subject: Witness Security Program
- (5) Detail all of the pertinent facts and circumstances; include the following information in the body of the memorandum:
 - a. State the nature of the investigation (that is, balance due account, delinquent return, periods, type of tax, amounts due, etc.)
 - b. List all collection actions taken to date.
 - c. List all facts indicating that the taxpayer is in the Witness Security Program.
 - d. List all identified assets and located assets.
 - e. State the NFTL determination; state if any NFTL was filed.
- (6) Send the memorandum, within three business days, to your GM via **secure** email.

- (7) If the GM concurs the taxpayer appears to be in WITSEC, the GM will forward the memorandum via secure email to the TM within three business days.
- (8) If the TM concurs the taxpayer appears to be in WITSEC, the TM will forward the memorandum via secure email to the WSC within three business days.

5.1.3.6.1.1
(09-23-2019)
**Witness Security
Coordinator Contact
Information**

- (1) The SB/SE WSC works in Operations Support, Business Support Office, Fraud Policy & Operations.
- (2) The WSC is the liaison between the IRS and the USMS.
- (3) The WSC email address is: **SBSE Witness Security Coordinator*

5.1.3.6.1.2
(09-23-2019)
**Witness Security
Coordinator Procedures**

- (1) This program requires sensitive handling. At no time will the WSC disclose if a taxpayer is in WITSEC.
- (2) If the USMS contacts the WSC, the WSC will identify the necessary steps to both protect the witness and address the outstanding tax issues and then provide those steps to the appropriate management level.
- (3) If the WSC receives a memo from a TM where the RO suspects a taxpayer is in WITSEC, the WSC will take the necessary actions to determine if the person is in WITSEC. The WSC will determine the necessary steps to protect the witness and address the outstanding tax issues, if applicable, and then provide those steps to the appropriate management level, including if normal collection actions may resume.

5.1.3.7
(12-15-2020)
Information Security

- (1) IRS employees must protect sensitive information at all times. Failure to protect sensitive information can result in disciplinary actions including admonishment, written reprimand, suspension, or removal. Sensitive information that requires protection includes any information that, if lost or disclosed, could violate a person's privacy, put a person at risk for identity theft, or compromise the integrity of the tax administration process. "IRS information" means Sensitive But Unclassified (SBU) information, which includes Federal tax returns and return information, Official Use Only information, Privacy Act information, and Personally Identifiable Information (PII). IRS employees and contractors are subject to Federal information security laws, regulations and policies including annual security awareness training which covers disclosure, privacy, UNAX, and computer security.
- (2) Protect any sensitive information that is entrusted to you pursuant to the applicable guidance in the following IRMs:
 - IRM 5.1.3.7.1, Information Gathering Guidelines
 - IRM 5.1.3.7.2, Personally Identifiable Information
 - IRM 5.1.3.7.3, Property and Records Protection
 - IRM 5.1.3.7.4, Privacy Act
 - IRM 5.1.3.7.5, Taxpayer Browsing Protection Act
- (3) Refer to the following IRMs if you require additional information:
 - a. IRM 10, Security, Privacy and Assurance, including IRM 10.2.1, Physical Security, IRM 10.5.8, Sensitive but Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments, and IRM 10.8.26, Wireless and Mobile Device Security Policy.

- b. IRM 11.3, Disclosure of Official Information, including IRM 11.3.1, Introduction to Disclosure, IRM 11.3.12, Designation of Documents, IRM 11.3.13, Freedom of Information Act, and IRM 10.5.6.2, Privacy Act General Provisions.

5.1.3.7.1
(09-23-2019)
**Information Gathering
Guidelines**

- (1) It is fundamental principle that ROs understand the parameters and limits for gathering information. Information gathering activities are controlled by the Privacy Act and third-party contact procedures. The applicable law and procedures, as they apply to ROs in FC, are discussed herein and in the following IRMs:

- IRM 25.27.1, Third-Party Contact Program
- IRM 5.1.22, Disclosure

5.1.3.7.1.1
(06-01-2010)
**Information Gathering
Procedures**

- (1) Gather the information you need according to the applicable law and procedures.
 - a. Seek only the information you need to administer, and when necessary, enforce the tax laws.
 - b. Consult with the local disclosure officer if you need assistance when questions arise concerning information gathering activities.

5.1.3.7.1.1.1
(09-23-2019)
**Gathering Information
from a Third-Party**

- (1) It is not necessary to obtain investigatory information directly from a taxpayer or the taxpayer's representative if doing so would impair an IRS investigation. Information may be obtained from third parties without soliciting such information directly from the taxpayer or the taxpayer's representative.
- (2) Follow the third-party contact rules whenever you contact a person other than the taxpayer regarding the determination or collection of the taxpayer's tax liability. See IRM 25.27.1, Third-Party Contact Program.
 - a. IRC 7602(c), Notice of contact of third parties, does not apply when the IRS is seeking information about groups of taxpayers (e.g., airline pilots or registered nurses.)
 - b. If your investigation focus shifts to determining or collecting an individual taxpayer's tax liability, then all the requirements of IRC 7602(c) must be met.

5.1.3.7.1.1.2
(09-23-2019)
**Notification About
Information Gathering**

- (1) A "system of records" is a group of records under the control of an agency from which information is retrieved by an individual's name, SSN, or other personal identifier. The Privacy Act requires Federal agencies to publish their Systems of Records (SOR) in the Federal Register. Any employee who maintains a system of records must meet the notice requirements in IRM 10.5.6.3, Privacy Act System of Records Notices (SORNs).
- (2) Follow the system of records procedures:
 - a. Do not index or associate any information with the name or identifying symbol of a taxpayer that is not required for the enforcement and administration of tax law.
 - b. Do not maintain background or historical files on taxpayers except when those files pertain to a currently assigned case.
 - c. Request your GM to authorize any exception for a specific purpose.

5.1.3.7.2
(06-06-2025)
**Personally Identifiable
Information**

- (1) PII must be protected. PII is a specific type of sensitive information that includes the personal data of taxpayers, IRS employees, contractors, job applicants, and visitors to IRS offices. PII is sensitive information that, either alone, or in combination with other information, can be used to uniquely identify, locate, or contact an individual. Specifically, the term “personally identifiable information” refers to information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc., either alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. IRM 10.5.1.2.3, Personally Identifiable Information (PII), provides a more comprehensive definition of PII.
- (2) PII includes:
 - Individual’s name and address,
 - Email address,
 - Telephone number,
 - Social security number,
 - Photographic images (specifically of face or other identifying characteristics), and
 - Biometric information (retina scans, voice signatures, or facial geometry.)
- (3) Some types of documents that contain SBU and PII are:
 - Payroll records
 - Personnel records
 - Financial records
 - Tax returns
- (4) Additional information sources about protecting PII and deterring identity theft include:
 - a. IRM 5.1.28, Identity Theft For Collection Employees
 - b. Contact Disclosure for answers regarding sending PII through email.

5.1.3.7.2.1
(09-23-2019)
Protecting PII

- (1) Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. Any loss of PII could result in the information being compromised to perpetrate identity theft. All IRS employees must take care to protect PII at all times, whether in paper form, or in IRS computer equipment and computer systems (including mobile computing devices.) PII information must be encrypted in email and when stored on computers. Sharing returns or return information with IRS co-workers is authorized only to the extent necessary for tax administration, i.e., “need to know.” Some work practices can also pose risks to the privacy of the information you handle on a daily basis, e.g., leaving sensitive information unattended on a printer or fax. You are responsible for protecting sensitive information in your office, at your home, on travel, and at a Telework / virtual office site. Managers and TIGTA may conduct random checks during or after business hours to ensure compliance with the “Clean Desk Policy.”
- (2) Examples of failures to properly protect sensitive information include:
 - a. Failure to encrypt electronic data and/or protect passwords.

- b. Failure to report any known or suspected loss of control or unauthorized disclosure of tax, tax return, or personally identifiable information.
 - c. Failure to properly safeguard paper documents.
 - d. Willful unauthorized disclosure.
 - e. Collection and maintenance of records without proper Privacy Act notice.
- (3) Check your desk, cabinets, briefcase, home office, laptop case, etc., for sensitive information in paper form.
 - a. Ensure paper files are securely stored (e.g., in locked file cabinets) when not in use.
 - b. Refer to IRM 10.5.1.5.1, Clean Desk Policy, for information about the policy.
- (4) Take care to safeguard and protect PII at all times, including encrypting PII information in email and on computers or portable electronic media.
 - a. Ensure electronic media are securely stored (e.g., in locked file cabinets) when not in use.
 - b. Encrypt sensitive information and PII that is processed, stored, or transmitted by computer equipment (such as laptops and memory storage devices).
 - c. Refer to IRM 10.8.26, Wireless and Mobile Device Security Policy, which establishes policy to implement the minimum security controls to safeguard IRS laptop computers.
 - d. Only release sensitive information and PII to those individuals having a “need-to-know” in the performance of their duties.

Reminder: Put PII away and lock it up.

5.1.3.7.2.1.1
(09-23-2019)
IRS Data Breaches

- (1) Sometimes, even when appropriate procedures have been followed, a loss of PII will occur, and a data breach will happen. When a taxpayer’s PII is lost due to a data breach and there is a likely risk of identity theft or other harm, the taxpayer will be notified by a letter from the IRS. All decisions to officially notify taxpayers of the loss of PII are done at the national level through Incident Management (IM). IM is located within the Office of Privacy, Governmental Liaison and Disclosure (PGLD), Office of Privacy Policy and Compliance. IM will send a Letter 4281C (or similar letter in special circumstances) to each taxpayer who is involved in a PII data breach if there is a likely risk of harm and the taxpayer can be identified. The letter will advise the taxpayer about available assistance, including the availability of a dedicated toll-free telephone number and the offer of free identity protection services.

Example: An RO spent part of the day making field calls. They properly stored their laptop computer and some hard-copy case files in their locked trunk so they could go into a restaurant for lunch. The laptop and the hard-copy case files were stolen from their automobile while the RO was eating lunch. The theft of the laptop and hardcopy case files constitutes a PII data breach. The RO will properly report both the theft of the laptop and the hardcopy documents as per IRM 5.1.3.7.2.1.1.2, Reporting a Potential Privacy or Data Breach, and will provide the SSNs of the affected individuals on the stolen hardcopy documents when requested by IM. IM will notify the taxpayers potentially impacted by the hardcopy document data breach since there is a likely risk of identity theft or other

harm. Notification will not be made for the individuals whose information was stored on the laptop since the laptop was appropriately encrypted.

5.1.3.7.2.1.1.1
(06-01-2010)
**Handling Calls from
Taxpayers**

- (1) Refer the taxpayer to the dedicated toll-free telephone number if you receive a telephone call from a taxpayer in response to one of the notification letters from IM. The dedicated toll-free phone number is 1-866-225-2009.

Note: The dedicated number is only for taxpayers who received a letter from IM.

5.1.3.7.2.1.1.2
(08-07-2024)
**Reporting a Potential
Privacy or Data Breach**

- (1) Report any potential privacy or data breach immediately if you suspect or know of a potential PII loss or a confirmed loss of sensitive information, such as a shipping loss or loss of a laptop, tax return, portable media, or “SmartID” badge, or if an unauthorized disclosure occurs. The first person who becomes aware of the loss is required to report it no later than one hour following the discovery of the loss or unauthorized disclosure.

- (2) Make a report immediately to the following, in the order listed:

1. Notify your manager.
2. Contact one of the following offices based on what was lost or disclosed: Office of Taxpayer Correspondence, PGLD IM Office or the Computer Security Incident Response Center (CSIRC). See IRM 10.5.4.3.3, Inadvertent Unauthorized Disclosures and Losses or Thefts of IT Assets, BYOD Assets and Hardcopy Records/Documents, for guidance about how to determine which office you should report to and how to contact each office.
3. Contact your local TIGTA office to report the theft of an IRS Information Technology (IT) asset or non-IRS IT asset (BYOD device), e.g., computer, laptop, router, printer, removable media, CD/DVD, flash drive, floppy, etc., or a loss or theft of hardcopy records/documents containing sensitive information, as well as *intentional* unauthorized disclosures, losses, and thefts. See IRM 5.1.3.4.4.1, Preferred Reporting Method to Contact TIGTA.

Note: Do not contact TIGTA for an *inadvertent* unauthorized disclosure.

- (3) Report lost property to TIGTA only if one of the following scenarios apply:

- The property was stolen.
- The property was found at a crime scene.
- The property was used in the commission of a crime.
- The property is law enforcement related (for example: radios, IRS CI law enforcement credentials, and IRS CI badges).
- The property is associated to be a high-risk data event by the IRS Computer Security Incident Response Center (CSIRC).

- (4) Contact the police, if applicable, and obtain a copy of the police report. Retain the copy in the case file.

Note: In addition to following the existing reporting procedures, once the RO has informed local management regarding the incident and local management has informed Area management, Area management must inform Collection Headquarters management regarding the incident.

5.1.3.7.3
(09-23-2019)**Property and Records Protection**

- (1) Employees will be held responsible for loss or theft of official records/documents if the loss or theft is attributable to negligence or carelessness.
- (2) Protect work related property and tax related records in your custody against loss, theft, fire, destruction, alteration, and unauthorized disclosure.
- (3) Keep work-related property and tax-related data under personal observation or in a locked container or room for protection:
 - a. while in a taxpayer's home or business location,
 - b. while in your home, or
 - c. while transporting the property between locations.
- (4) Do not leave work items, especially remittances, unattended, even in IRS offices, to prevent theft and unauthorized disclosure. Refer to IRM 5.1.2, Remittances, Form 809 and Designated Payments, for guidance regarding converting cash payments to a bank draft or money order by the close of the business day on which it is collected, or as soon as possible on the next business day.
- (5) Exercise judgment when deciding to store the work items in a car. When work-related property and tax-related data needs to be kept in a car, lock the items in the trunk and lock the car. Take necessary precautions to ensure proper security if the car does not seem to afford adequate protection.
- (6) Refer to IRM Part 10, Security, Privacy and Assurance, including IRM 10.8.26, Wireless and Mobile Device Security Policy, to determine the type and degree of protection to be afforded to items related to FC activity.
- (7) All employees have the responsibility for ensuring IRS records, in hard copy and electronic format, are appropriately managed, retained, and archived in accordance with the National Archives and Records Administration approved records retention and disposition authority. Refer to series IRM 1.15, Records and Information Management, for compliance with records and files management lifecycle (hardcopy and electronic), including creation, maintenance, retrieval, preservation and disposition of all records to avoid inadvertent/unlawful destruction of records.

5.1.3.7.4
(08-07-2024)**Privacy Act**

- (1) The Privacy Act guarantees each individual certain protections for the personal information that the Federal government collects whenever an individual is requested to provide tax information in a non-criminal investigation to carry out the U.S. tax laws and collect the right amount of tax. The Privacy Act applies to individuals acting in an entrepreneurial capacity, such as a sole proprietorship, as well as individuals personally.
- (2) The Privacy Act requires the IRS to provide certain information to a taxpayer when we ask for information.
- (3) Notice 609, Privacy Act Notice, was developed to provide the Privacy Act notification. Notice 609 informs individuals of their privacy rights in non-criminal cases and is automatically sent to individuals with the Individual Master File (IMF) delinquency first notice.
- (4) Many forms, letters, and publications have been revised to contain the Privacy Act notification, however, but not all have been revised. Some IRS paper products (for example, a form or a return) contain only a reference to the

Privacy Act, if not the complete text of the Privacy Act Notice. It is not necessary to provide Notice 609 to an individual if the Privacy Act Notice language is included or referenced in the text of the IRS paper product you are requesting the individual to complete.

Example: Form 433-A and Form 433-B say:

“Privacy Act: The information requested on this Form is covered under Privacy Acts and Paperwork Reduction Notices which have already been provided to the taxpayer.” You are not required to supply Notice 609 to the taxpayer with Form 433-A and/or Form 433-B.

Example: At the bottom of Form 4180, Report of Interview of Individual, is a box labeled “Interview Handouts” which is to be checked if Notice 609 is given during the interview. If Notice 609 is not given during the interview, the interviewer is to explain why not in the case history. One possible explanation is that the individual received a copy of Notice 609 at a previous interview or contact.

- (5) Refer to IRM 10.5.6, Privacy Act, if you require additional information. It discusses the Privacy Act, the basic principles of privacy, and among other things, the IRS’s commitment to protecting privacy.

5.1.3.7.4.1
(09-23-2019)
**Privacy Act Notification
Procedures**

- (1) Provide Notice 609 as notification of the Privacy Act to a taxpayer to inform them of their right to privacy when you ask for tax information from the taxpayer in a non-criminal investigation such as a Trust Fund Recovery Penalty (TFRP) investigation:
 - a. When hand-delivering any first notice on a prompt, quick, jeopardy, or termination assessment on an individual,
 - b. On all initial Compliance Initiative Program contacts with an IMF taxpayer, and
 - c. In all other contact situations when requesting personal information from an individual unless you have already notified the individual regarding the Privacy Act.

Example: IRM 5.7.4.2.4, Form 4180, requires Notice 609 to be provided to an individual during a TFRP investigation interview.

- (2) Mail Notice 609 to the taxpayer in a separate envelope when you cannot include it in the envelope with any other correspondence directed to the taxpayer if the forms and publications you are sending do not contain the Privacy Act Notice.

5.1.3.7.5
(06-01-2010)
**Taxpayer Browsing
Protection Act**

- (1) The Taxpayer Browsing Protection Act (Public Law 105-35) (the Act) amended the Internal Revenue Code of 1986 to prohibit the willful unauthorized access or inspection of tax returns and return information. The Act added IRC 7213A, Unauthorized inspection of returns or return information, which designated willful unauthorized access or inspection of any taxpayer records as a criminal offense. The Act is commonly known as UNAX. Unauthorized access could lead to dismissal of an IRS employee in accordance with the Act.

5.1.3.7.5.1
(06-06-2025)

The UNAX Program

- (1) The mission of the UNAX Program is to:
 - Provide UNAX awareness to all IRS employees.
 - Prevent unauthorized access to and inspection of taxpayer information.
 - Ensure that employees do not compromise public confidence in our protection of tax account information.
- (2) See IRM 10.5.5, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance, and Requirements for further information about the UNAX Program.

5.1.3.7.5.1.1
(09-23-2019)

**UNAX Procedures —
Form 11377**

- (1) Form 11377, Taxpayer Data Access, was implemented to provide a way for employees to document various situations.
- (2) Use Form 11377 or Form 11377-E to:
 - Document access to taxpayer return information when the access is not supported by direct case assignment.
 - Document an access performed in error.
 - Document an access that may raise a suspicion of an unauthorized access.

Reminder: Use Form 11377-E for electronic completion/submission.

- (3) Follow the instructions included on Form 11377 and Form 11377-E to complete the form. The instructions also include directions for managers to submit the form to their Business Unit Head of Office Designee. See the UNAX website for a contact list of Business Unit Head of Office Designees.

5.1.3.8
(09-23-2019)

Internal Control

- (1) All personnel have responsibility for understanding and ensuring that internal controls are functioning as intended. Internal control:
 - a. Is a major part of managing an organization comprising the plans, methods, and procedures used to meet missions, goals, and objectives.
 - b. Serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud.
- (2) Refer to IRM 1.4.2, Monitoring and Improving Internal Control, for additional information regarding the establishment and maintenance of adequate internal control systems based on law and regulations.

5.1.3.8.1
(09-23-2019)

Separation of Duties

- (1) Separation of duties is a key component of internal control; this IRM section provides guidance on separation of duties for FC employees. With separation of duties, each person in a transaction provides a check over the other person when two components of a transaction are processed by different individuals. Separation of duties:
 - a. Requires multiple individuals to perform key duties and responsibilities.
 - b. Requires authorizing, processing, recording, and reviewing transactions to be separated among individuals.
 - c. Acts as a deterrent to fraud and concealment.
 - d. Deters collusion by one individual with another individual to complete a fraudulent act.
- (2) The following examples demonstrate the concept of separation of duties:

Example: An RO receives a payment, completes Form 3244, Payment Posting Voucher, and transmits the voucher and payment to the campus. An employee in Submission Processing processes the payment.

Example: An RO receives an original return filed to replace a substitute for return assessment, completes Form 3870, Request for Adjustment, and transmits the request for reconsideration to the campus. An employee in SB/SE Service Centers — Compliance Services processes the request for reconsideration.

Example: An RO receives a cash payment from a taxpayer and issues Form 809, Receipt for Payment of Taxes, to the taxpayer; the receipt shows the amount of cash received from the taxpayer. The RO converts the cash, and transmits the remittance (i.e., a check or money order in the amount of cash received from the taxpayer) along with the Form 809 to the campus. An employee in Submission Processing processes the payment for credit to the taxpayer's account (in the amount of cash received from the taxpayer) and ensures deposit to the Treasury. .

Note: IRM 5.1.2, Remittances, Form 809, and Designated Payments, provides guidance regarding converting cash payments to a bank draft or money order

(3) Ensure separation of duties as you perform your work as an RO.

This Page Intentionally Left Blank

Exhibit 5.1.3-1 (09-23-2019)

Armed Escort Requests- Minimum Required Information

Requests for all armed escorts must include the following information:

PDT	CAU	Other
(blank)	***IMPORTANT***	(blank)
Contact TIGTA's Office of Investigations directly if an armed escort is being considered for a taxpayer designated a PDT.	Prior to submitting this request, the requesting IRS employee/ management official must contact OEP and obtain the basis for OEP's CAU designation.	IRS management must evaluate this situation and if it is decided an armed escort is still required proceed with contacting TIGTA's Office of Investigations.
(blank)	***IRS management must evaluate this information and if it is decided an armed escort is still required proceed with the memorandum.***	(blank)
Subject's name	Subject's name	Subject's name
Home address	Home address	Home address
Social Security number	Social Security number	Social Security number
Contact number(s)	Contact number(s)	Contact number(s)
(blank)	(blank)	If subject is an IRS employee/ contractor provide position, grade, function and POD information
Assigned IRS employee's name, position and contact information (provide a description or photo of the employee)	Assigned IRS employee's name, position and contact information (provide a description or photo of the employee)	Assigned IRS employee/ management official's name, position and contact information (provide a description or photo of the employee)
PDT designation – yes or no	CAU designation – yes or no	(blank)
(blank)	Basis for OEP CAU designation	Background information concerning subject
Description of the tax issue	Description of the tax issue	(blank)
Description of activity to take place and time/date of activity	Description of activity to take place and time/date of activity	Description of activity to take place and time/date of activity
Number of IRS employees/ others who will attend	Number of IRS employees/ others who will attend	Number of IRS employees/ management officials/others who will attend
Location of activity, detailed description of location or business, type of activity at the location, and any other individuals likely to be present	Location of activity, detailed description of location or business, type of activity at the location, and any other individuals likely to be present	Location of activity, detailed description of location or business, type of activity at the location, and any other individuals likely to be present

Exhibit 5.1.3-1 (Cont. 1) (09-23-2019)**Armed Escort Requests- Minimum Required Information**

PDT	CAU	Other
Physical description of taxpayer	Physical description of taxpayer	Physical description of taxpayer
IRS employee knowledge of any weapons owned by the taxpayer or any military or weapons training	IRS employee knowledge of any weapons owned by the taxpayer or any military or weapons training	IRS employee knowledge of any weapons owned by the taxpayer or any military or weapons training
Any contact or statements related to the subject that caused concern	Any contact or statements related to the subject that caused concern	Any contact or statements related to the subject that caused concern
Any other information obtained related to the subject that would indicate an armed escort is warranted	Any other information obtained related to the subject that would indicate an armed escort is warranted	Any other information obtained related to the subject that would indicate an armed escort is warranted