



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

13.10.2

SEPTEMBER 9, 2025

EFFECTIVE DATE

(09-09-2025)

PURPOSE

- (1) This transmits new IRM 13.10.2, Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls, Maintaining Internal Controls.

MATERIAL CHANGES

- (1) This transmits new IRM 13.10.2, Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls.
- (2) The following table identifies the subsections that were moved from IRM 1.4.13 into IRM 13.10.2 as all TAS employees are responsible for internal controls, not just managers. In addition, the table identifies any additional material changes that were made to the subsections since the last published revision of these sections:

Current IRM Subsection	Former IRM Subsection	Other Material changes made to the subsection.
IRM 13.10.2.1, Program Scope and Objectives	IRM 1.4.13.4, Maintaining Internal Controls	
IRM 13.10.2.1.1, Authority	IRM 1.4.13.4.1, Federal Managers' Financial Integrity Act	
IRM 13.10.2.1.2, Responsibilities	IRM 1.4.13.4.2, Roles and Responsibilities	
IRM 13.10.2.1.3, Program Management and Review	IRM 1.4.13.4.3, Internal Controls Managerial Assessment	<ul style="list-style-type: none">• Removed "individual online" since the assessments are not all done online.• Removed (3-5) due to changes to the ICMA process
IRM 13.10.2.1.4, Terms	1.4.13-1, Terms	Removed TAMIS and SAMS due to Phoenix
IRM 13.10.2.1.5, Acronyms	1.4.13-1, Acronyms	Removed TAMIS and SAMS due to Phoenix
IRM 13.10.2.1.6, Related Resources	IRM 1.4.13.4.4, Internal Controls Resources	

IRM 13.10.2.2.1, Manual Refunds	IRM 1.4.13.4.5, Manual Refunds	<ul style="list-style-type: none">• Replaced reference to the TAS Manager Handbook with a cross reference to IRM 1.4.13.9.6.4.6(5) where information is currently located. IPU 23U0733 issued 6-15-2023.• Added additional cross references and added a note concerning manual monitoring for manual refunds input after June 16, 2023. IPU 23U0856 issued 07-28-2023.• Updated to remove manual refund monitoring requirements per IRM 21.4.4.6.1, Monitoring Manual Refunds. IPU 23U1134 issued 11-29-2023.• Updated citation to IRM 10.8.34.10.2.1.6.8, Automated Command Code Access Control.• Removed“ If an LTA in another office approved and signed the manual refund, the initiator’s manager is still response for this review.”, this pertains to review that are no longer required.
---------------------------------	--------------------------------	--

IRM 13.10.2.2.1.1, Manual Refunds Training	IRM 1.4.13.4.5.1, Manual Refunds Training	<ul style="list-style-type: none"> Updated for consistency with training requirements for employees initiating, reviewing, signing, and monitoring manual refunds in IRM 3.17.79.1.1.1. Per IRM 21.4.4.6.1(1) (6/15/2023), effective June 20, 2023, do not add any manual refunds into the EMT/Case Monitoring Tool. Monitoring will continue for those manual refunds input before June 20, 2023. Added a note concerning manual monitoring for manual refunds input after June 16, 2023. IPU 23U0856 issued 07-28-2023. Updated to correct training requirements per IRM 3.17.79.1.1.1, Training, and removed training related to manual refund monitoring as manual refund monitoring per IRM 21.4.4.6.1, Monitoring Manual refunds. IPU 23U1134 issued 11-29-2023. Removed paragraph (2) training is no longer required for manual refund reviewers.
IRM 13.10.2.2.2, Payment Processing	IRM 1.4.13.4.6, Payment Processing	<ul style="list-style-type: none"> Clarified that TAS does not generally accept any form of payment from taxpayers.
IRM 13.10.2.2.3, Return Processing	IRM 1.4.13.4.7, Return Processing	<ul style="list-style-type: none"> Added a link to IRM 13.1.24.6.2.7.1, Time Sensitive Unprocessed Original Return Procedures.
IRM 13.10.2.2.4, IDRS	IRM 1.4.13.4.8, IDRS	

IRM 13.10.2.2.4.1, IDRS Security	IRM 1.4.13.4.8.1, IDRS Security	<ul style="list-style-type: none"> Clarified that Case Advocacy Specialists are included in the Research Profile Type for IDRS. IPU 23U0733 issued 6-15-2023. Clarified managers are required to advise users with 15 or more systemic sign-offs in one month of the expectation to properly sign-off when away from their workstations or not actively using IDRS. Clarified IDRS users with Full Access profiles are required to CMODE out of Andover to the designated IMF and BMF office and have the Null feature set to "On".
IRM 13.10.2.2.4.1.1, Making Deviations from an IDRS MPAF and RSTRK Definer U	1.4.13.4.8.1.1, Making Deviations from an IDRS MPAF and RSTRK Definer U	<ul style="list-style-type: none"> Updated to incorporate tracking procedures for the IDRS Deviation Tracking Sheet.
IRM 13.10.2.2.4.2, Authorized IDRS Access	IRM 1.4.13.4.8.2, Authorized IDRS Access	<ul style="list-style-type: none"> Updated to clarify procedures for Form 11377-E. (5) Added a note concerning the use of Taxpayer Identification Numbers (TINs). (6) Added a new bullet to ensure TINs are redacted from Form 11377-E supporting documents.
IRM 13.10.2.2.4.2.1, IDRS Access of an IRS Employee Account		<ul style="list-style-type: none"> Updated to clarify when a Form 11377-E, Taxpayer Data Access, should be completed when an inquiry or case concerns an IRS employee. IPU 23U1134 issued 11-29-2023.
IRM 13.10.2.2.4.3, IDRS Retention Criteria	IRM 1.4.13.4.8.3, IDRS Retention Criteria	
IRM 13.10.2.2.4.4, IDRS Message File	IRM 1.4.13.4.8.4, IDRS Message File	

IRM 13.10.2.2.4.5, Manager Responsibilities	IRM 1.4.13.4.8.5, Manager Responsibilities	<ul style="list-style-type: none"> Updated reference to IRM 10.5.5.3.5. IPU 23U0733 issued 6-15-2023. Moved procedures concerning Form 11377-E to IRM 13.10.2.2.4.2 and added a cross reference to that section. Updated cross references.
IRM 13.10.2.2.4.6, Reviewers of IDRS Adjustments	IRM 1.4.13.4.8.6, Reviewers of IDRS Adjustments	<ul style="list-style-type: none"> Updated language to specify which transactions should be 100% reviewed for all other employees. Moved (5) to (7) and added "For transactions input over the weekend". Removed last sentence in (6) since USRs are required to add their IDRS unit numbers to the EOD 02 file. Added "two days" to (6) to specify the time frame of the suspension.
IRM 13.10.2.2.4.7, Unit Security Representative Responsibilities	IRM 1.4.13.4.8.7, Unit Security Representative Responsibilities	<ul style="list-style-type: none"> Updated reference to IRM 10.8.34.2.1.3. IPU 23U0733 issued 6-15-2023. Updated cross references throughout.
IRM 13.10.2.2.4.8, Terminal Security Administrator	IRM 1.4.13.4.8.8, Terminal Security Administrator	
IRM 13.10.2.2.4.9, TAS IORS POC Responsibilities	IRM 1.4.13.4.8.9, TAS IORS POC Responsibilities	<ul style="list-style-type: none"> Updated references to IRM 10.5.5.3.5, IRM 10.8.34.2.2.5 and IRM 10.8.34.5.3.1. IPU 23U0733 issued 6-15-2023.
IRM 13.10.2.2.4.10, TAS IDRS Business Unit POC Responsibilities	IRM 1.4.13.4.8.10, TAS IDRS Business Unit POC Responsibilities	

IRM 13.10.2.2.5, TAS Systems Access	IRM 1.4.13.4.9, TAS Systems Access	<ul style="list-style-type: none"> Removed link to the TAS Security and New Hire Equipment and Software Requests as these are no longer available. Updated title of TAS Technology Place to TAS Technology Hub. IPU 23U0733 issued 6-15-2023.
IRM 13.10.2.2.5.1, Reserved	IRM 1.4.13.4.9.1, TAMIS	Changed "TAMIS" to "Reserved". Will update when Phoenix goes live.
Removed	IRM 1.4.13.4.9.1.1, Making Deviations from a TAMIS Permission Level	This section was removed. Will revisit when Phoenix goes live.
IRM 13.10.2.2.5.2, Reserved	IRM 1.4.13.4.9.2, Systemic Advocacy Management System (SAMS)	Changed "SAMS" to "Reserved". Will update when Phoenix goes live.
IRM 13.10.2.2.6, Clean Desk Policy	IRM 1.4.13.4.10, Clean Desk Policy	
IRM 13.10.2.2.7, Confidentiality of Tax Returns and Tax Return Information	IRM 1.4.13.4.11, Confidentiality of Tax Returns and Tax Return Information	<ul style="list-style-type: none"> Added a cross reference to the TIGTA website.
IRM 13.10.2.2.8, Disclosure	IRM 1.4.13.4.16, Disclosure	
IRM 13.10.2.2.11, TAS Space Requirements	TAS Manager Handbook, Chapter 5(I)	<ul style="list-style-type: none"> Updated to current policies.
IRM 13.10.2.2.11.1, Local Point of Contact (LPOC) Responsibilities	TAS Manager Handbook, Chapter 5(I)(i)	<ul style="list-style-type: none"> Updated to current policies.
Exhibit 13.10.2-1, IDRS MPAF for Case Advocates (Including Lead Case Advocates)	Exhibit 1.4.13-4, IDRS MPAF for Case Advocates (Including Lead Case Advocates)	<ul style="list-style-type: none"> Removed Command Code (CC) EFTOF. TAS employees do not have the delegated authority to input skip payments on DDIA's, since this CC is solely used to input skip payments for DDIA's it has been removed. IPU 23U1134 issued 11-29-2023. Removed Command Code (CC) FTPIN. CC INTSTD replaced FTPIN.

Exhibit 13.10.2-2, IDRS MPAF for Intake Advocates (Including Lead Intake Advocates)	Exhibit 1.4.13-5, IDRS MPAF for Intake Advocates (Including Lead Intake Advocates)	<ul style="list-style-type: none"> Removed Command Code (CC) FTPIN. CC INTSTD replaced FTPIN. Corrected CC RPFTP to RTFTP
Exhibit 13.10.2-3, IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors	Exhibit 1.4.13-6, IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors	<ul style="list-style-type: none"> Clarified the title by adding Case Advocacy Specialists. IPU 23U0733 issued 6-15-2023. Removed CCs STAUP, STATB, and STATI as these CCs conflict with IRM 10.8.34-11 where anyone with RSTRKU on their profile cannot have these CCs. Removed Command Code (CC) FTPIN. CC INTSTD replaced FTPIN. Added CC FTDPN. Used to research FTD penalties. Corrected CC RPFTP to RTFTP
Exhibit 13.10.2-4, IDRS MPAF for Quality Analysts	Exhibit 1.4.13-7, IDRS MPAF for Quality Analysts	<ul style="list-style-type: none"> Removed Command Code (CC) FTPIN. CC INTSTD replaced FTPIN. Corrected CC RPFTP to RTFTP
Exhibit 13.10.2-5, IDRS MPAF for TAS Managers	Exhibit 1.4.13-8, IDRS MPAF for TAS Managers	<ul style="list-style-type: none"> Added command code (CC) COMPA as managers use it to verify calculations. IPU 23U0733 issued 6-15-2023. Removed Command Code (CC) FTPIN. CC INTSTD replaced FTPIN. Added CC FTDPN. Used to research FTD penalties. Corrected CC RPFTP to RTFTP
Exhibit 13.10.2-6, Command Codes for IDRS Online Reviews of Account Adjustments	Exhibit 1.4.13-9, Command Codes for IDRS Online Reviews of Account Adjustments	
Exhibit 13.10.2-7, Security Command Codes for Unit Security Representatives	Exhibit 1.4.13-10, Security Command Codes for Unit Security Representatives	
Exhibit 13.10.2-8, Security Command Codes for Terminal Security Administrators	Exhibit 1.4.13-11, Security Command Codes for Terminal Security Administrators	

Exhibit 13.10.2-9, IDRS Multiple Access Approval Table	Exhibit 1.4.13-12, IDRS Multiple Access Approval Table	<ul style="list-style-type: none"> • Added reactivated unit 63861 to 1-Andover. IPU 23U0856 issued 07-28-2023. • Added reactivated unit 63261 to Pittsburgh, 63258 to Charlotte, and 63212 to Greensboro. • Added unit 63127-63129 to ITAP. Also, removed unit 63822 to ITAP. • Added unit 63712 for Oakland. • Removed unit 63630 from Area 5 Oklahoma City. • Added unit 63561 to Area 7, Phoenix. • Updated unit 63382 from EDCA-ITS, CCI Fresno to EDCA-ITS, CCI Puerto Rico. • Updated St. Petersburg to Clearwater. • Updated to correct the IDRS unit code for Quality Review Program to 63714 and Northern Kentucky to Covington. IPU 24U0376 issued 3-8-2024. • Updated to include a cross reference to IRM 13.10.2.2.4.1(6). • Updated to assign IDRS Unit Number 63487 to TAS IORS POC and TAS IDRS Analysts. • Updated to include AU as a campus for manual refunds per IRM 3.17.79.3.5.
--	--	--

EFFECT ON OTHER DOCUMENTS

Procedures previously found in IRM 1.4.13.5, Maintaining Internal Controls; Exhibit 1.4.13-4, IDRS MPAF for Case Advocates (Including Lead Case Advocates); Exhibit 1.4.13-5, IDRS MPAF for Intake Advocates (Including Lead Intake Advocates); Exhibit 1.4.13-6, IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors; Exhibit 1.4.13-7, IDRS MPAF for Quality Analysts; Exhibit 1.4.13-8, IDRS MPAF for TAS Managers; Exhibit 1.4.13-9, Command Codes for IDRS Online Reviews of Account Adjustments; Exhibit 1.4.13-10, Security Command Codes for Unit Security Representatives; Exhibit 1.4.13-11, Security Command Codes for Terminal Security Administrators; and Exhibit 1.4.13-12, IDRS Multiple Access Approval Table, have been incorporated into this IRM section.

AUDIENCE

Taxpayer Advocate Service employees

Elizabeth R. Blazey-Pennel

Acting Executive Director Case Advocacy, Intake and Technical
Support

13.10.2

Maintaining Internal Controls

Table of Contents

13.10.2.1 Program Scope and Objectives

13.10.2.1.1 Authority

13.10.2.1.2 Responsibilities

13.10.2.1.3 Program Management and Review

13.10.2.1.4 Terms

13.10.2.1.5 Acronyms

13.10.2.1.6 Related Resources

13.10.2.2 Maintaining Internal Controls

13.10.2.2.1 Manual Refunds

13.10.2.2.1.1 Manual Refund Training

13.10.2.2.2 Payment Processing

13.10.2.2.3 Return Processing

13.10.2.2.4 Integrated Data Retrieval System (IDRS)

13.10.2.2.4.1 IDRS Security

13.10.2.2.4.1.1 Making Deviations From an IDRS MPAF and RSTRK Definer U

13.10.2.2.4.2 Authorized IDRS Access

13.10.2.2.4.2.1 IDRS Access of an IRS Employee Account

13.10.2.2.4.3 IDRS Retention Criteria

13.10.2.2.4.4 IDRS Message File

13.10.2.2.4.5 Manager Responsibilities

13.10.2.2.4.6 Reviewers of IDRS Adjustments

13.10.2.2.4.7 Unit Security Representative Responsibilities

13.10.2.2.4.8 Terminal Security Administrator (TSA)

13.10.2.2.4.9 TAS IORS POC Responsibilities

13.10.2.2.4.10 TAS IDRS Business Unit POC Responsibilities

13.10.2.2.5 TAS Systems Access

13.10.2.2.5.1 Reserved

13.10.2.2.5.2 Reserved

13.10.2.2.6 Clean Desk Policy

13.10.2.2.7 Confidentiality of Tax Returns and Tax Return Information

13.10.2.2.8 Disclosure

13.10.2.2.9 Records Retention

13.10.2.2.10 Financial Guidelines

13.10.2.2.11 TAS Space Requirements

13.10.2.2.11.1 Local Point of Contact (LPOC) Responsibilities

Exhibits

- 13.10.2-1 IDRS MPAF for Case Advocates (Including Lead Case Advocates)
- 13.10.2-2 IDRS MPAF for Intake Advocates (Including Lead Intake Advocates)
- 13.10.2-3 IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors
- 13.10.2-4 IDRS MPAF for Quality Analysts
- 13.10.2-5 IDRS MPAF for TAS Managers
- 13.10.2-6 Command Codes for IDRS Online Reviews of Account Adjustments
- 13.10.2-7 Security Command Codes for Unit Security Representatives
- 13.10.2-8 Security Command Codes for Terminal Security Administrators
- 13.10.2-9 IDRS Multiple Access Approval Table

13.10.2.1
(09-09-2025)
Program Scope and Objectives

- (1) This section supplements IRM 1.4.2, Monitoring and Improving Internal Control, and provides Taxpayer Advocate Service (TAS) managers and employees with TAS-specific guidelines, methods, and techniques for maintaining internal controls. Internal controls are the programs, policies, and procedures established to ensure TAS:
 - a. Efficiently and effectively carries out its mission and program objectives.
 - b. Protects programs and resources from waste, fraud, abuse, mismanagement, and misappropriation of funds.
 - c. Follows laws and regulations.
 - d. Ensures financial reporting is reliable.
 - e. Obtains reliable information and uses it when making decisions.
- (2) *Purpose:* Internal controls are everyone's responsibility. This guidance applies to all TAS employees. In addition, TAS expects managers to understand the risks associated with their operations, to ensure controls are in place and operating effectively to mitigate known risks, and to provide candid, reliable, and supportable annual reports on the status of those controls. For more information, see IRM 1.4.2, Resource Guide for Managers, Monitoring and Improving Internal Control.
- (3) *Audience:* These procedures apply to all TAS employees.
- (4) *Policy Owner:* The Deputy National Taxpayer Advocate (DNTA), who reports to the National Taxpayer Advocate.
- (5) *Program Owner:* The Executive Director Case Advocacy, Intake & Technical Support (EDCA-ITS), who reports to the DNTA.

13.10.2.1.1
(09-09-2025)
Authority

- (1) Section 113 of the Budget and Accounting Procedures Act of 1950, Public Law 81-785, requires the head of each federal department and agency to establish and maintain adequate systems of management controls. Further, the Federal Managers' Financial Integrity Act of 1982, Public Law 97-255 (hereinafter "FMFIA"), requires each executive agency to establish internal accounting and administrative controls in accordance with standards prescribed by the Comptroller General. See IRM 1.4.2.1.2, Authorities, for more information.
- (2) The IRS and TAS are required to maintain an effective internal control program that complies with legislative requirements and related regulations and directives, such as the *Standards for Internal Control in the Federal Government*, commonly known as the "Green Book," issued by the U.S. Government Accountability Office (GAO).

13.10.2.1.2
(09-09-2025)
Responsibilities

- (1) The National Taxpayer Advocate is responsible for:
 - a. Establishing adequate and effective controls for all operations and activities in TAS's area of mission responsibility.
 - b. Ensuring the entire organization follows established controls.
 - c. Conducting a self-assessment and reporting on the status of internal controls in the organization to the Management Controls Executive Steering Committee (MC ESC) annually. Managers throughout the IRS are responsible for participating in this annual assessment in accordance with the annual guidance issued.
 - d. Evaluating reports of significant deficiencies and providing comments to the MC ESC.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

- e. Providing adequate resources to correct identified material weaknesses and significant deficiencies.
- f. Designating an Internal Control Coordinator to serve as a single point of contact for the assurance process and for FMFIA corrective actions and audit follow-up for their organization.
- g. Preparing executive summaries for agenda topics at MC ESC meetings.

(2) All TAS managers are responsible for:

- a. Providing a positive control environment;
- b. Identifying potential risk areas;
- c. Ensuring adequate and effective controls are in place;
- d. Reporting results of reviews to the next level of management;
- e. Ensuring reports are supportable, accurate, and candid;
- f. Providing adequate resources to correct identified problems;
- g. Implementing corrective actions timely; and
- h. Validating outcomes.

(3) All TAS employees are responsible for:

- a. Fulfilling the duties and responsibilities established in their position descriptions and meeting applicable performance standards.
- b. Taking all reasonable steps to safeguard assets and resources against waste, loss, damage, unauthorized use, or misappropriation.
- c. Reporting breakdowns in internal control systems or suggesting improvements to their manager.

13.10.2.1.3 (09-09-2025)

Program Management and Review

- (1) All managers conduct an annual self-assessment whereby they must review the effectiveness of controls within their own area of responsibility. Managers document these self-assessments by completing the Internal Controls Managerial Assessment (ICMA).
- (2) The ICMA focuses on the adequacy of internal controls within each organization. Managers assess risks (*i.e.*, the probability of a negative, unanticipated occurrence) of operations, determine if controls mitigate those risks, and certify those controls are effective. If not, managers will identify significant deficiencies found in the internal control procedures. See IRM 1.4.2.2.2, Annual Assurance Review Process, for more information.

13.10.2.1.4 (09-09-2025)

Terms

- (1) The following table provides terms and definitions used throughout this IRM.

Term	Definition
Improvement	The pursuit of opportunities to improve tax administration for the benefit of taxpayers.

Term	Definition
Internal Controls	<p>Internal controls are the programs, policies, and procedures established to ensure TAS:</p> <ul style="list-style-type: none"> a. Efficiently and effectively carries out its mission and program objectives. b. Protects programs and resources from waste, fraud, abuse, mismanagement, and misappropriation of funds. c. Follows laws and regulations. d. Ensures financial reporting is reliable. e. Obtains reliable information and uses it when making decisions.

13.10.2.1.5
(09-09-2025)
Acronyms

(1) The following table provides acronyms used throughout this IRM.

Acronym	Definition
ATA	Account Technical Advisor
BEARS	Business Entitlement Access Request System
BU	Bargaining Unit
CC	Command Code
CCI	Centralized Case Intake
CFOL	Corporate Files On-line
DDIA	Direct Debit Installment Agreement
DEDSA	Deputy Executive Director Systemic Advocacy
Deputy	Deputy Executive Director Case Advocacy
DNTA	Deputy National Taxpayer Advocate
EDCA	Executive Director Case Advocacy
EDCA-ITS	Executive Director Case Advocacy, Intake & Technical Support

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Acronym	Definition
EDSA	Executive Director Systemic Advocacy
FHC	Finance and Human Capital
FMFIA	Federal Managers' Financial Integrity Act of 1982
GPRA	Government Performance and Results Act
ICMA	Internal Controls Managerial Assessment
IDRS	Integrated Data Retrieval System
IOIRS	IDRS Online Reports Services
IA	Intake Advocate
IT	Information Technology
ITAP	Internal Technical Advisor Program
ITM	Integrated Talent Management
LCA	Lead Case Advocate
LIA	Lead Intake Advocate
LTA	Local Taxpayer Advocate
LPOC	Local Point of Contact
MC ESC	Management Controls Executive Steering Committee
MPAF	Maximum Profile Authorization File
MR	Manual Refund
NBU	Non-Bargaining Unit
OMB	Office of Management and Budget
POC	Point of Contact
TAG	Technical Analysis and Guidance
TAGM	Taxpayer Advocate Group Manager
TAS	Taxpayer Advocate Service
TIF	Taxpayer Information Files
TIN	Taxpayer Identification Number

Acronym	Definition
TIGTA	Treasure Inspector General for Tax Administration
TSA	Terminal Security Administrator
UNAX	Unauthorized Access
USR	Unit Security Representative

13.10.2.1.6
(09-09-2025)

Related Resources

- (1) The following statutes and regulations are the most significant authorities that affect the management controls program at the IRS:
 - a. Federal Managers' Financial Integrity Act (FMFIA) of 1982;
 - b. Federal Financial Management Improvement Act of 1996;
 - c. Chief Financial Officers Act of 1990;
 - d. *OMB Circular A-123*, Management's Responsibility for Enterprise Risk Management and Internal Control;
 - e. *Treasury Directive 40-04*, Treasury Internal Control Program;
 - f. Inspector General Act of 1978, as amended;
 - g. GAO, *Standards for Internal Control in the Federal Government* (the "Green Book");
 - h. Government Performance and Results Act (GPRA) Modernization Act of 2010;
 - i. IRM 1.4.2, Monitoring and Improving Internal Control;
 - j. IRM 1.4.3, Financial Assurance Control Testing;
 - k. IRM 1.4.32, Internal Control Review Program;
 - l. IRM 1.5.1, The IRS Balanced Performance Measurement System; and
 - m. IRM 13.5.1, TAS Balanced Performance Measurement System.

13.10.2.2
(09-09-2025)

Maintaining Internal Controls

- (1) TAS employees will use the procedures provided in the following subsections in conjunction with other TAS and IRS guidance to maintain internal controls.

13.10.2.2.1
(09-09-2025)

Manual Refunds

- (1) The purpose of issuing a manual refund is to provide the taxpayer quick access to overpayments and credits. See IRM 21.4.4.3, *Why Would a Manual Refund be Needed?*, for details about when a manual refund may be necessary. Normal computer processing does not generate a manual refund. It requires special preparation to allow the refunds release under unusual circumstances. This preparation includes suppressing the normal computer processes that automatically refund overpayments to prevent the taxpayer from receiving two refunds for the same overpayment. Management is responsible for ensuring employees take all actions to avoid the issuance of a duplicate erroneous refund.
- (2) Initiators of manual refunds are required to research for potential duplicate refunds. See IRM 21.4.4.5, *Preparation of Manual Refund Forms*.
 - a. In situations where initiators of manual refunds cannot obtain documentation of the taxpayer's hardship, they should have a discussion with the Local Taxpayer Advocate (LTA). The LTA can substitute a signed

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

statement that must contain a description of the hardship and the actions taken to verify the hardship. See IRM 3.17.79.3.3(2), Issuing Hardship Refunds.

- (3) Only LTAs (or LTAs acting 60 days or more) may approve manual refunds.
 - a. LTAs (or LTAs acting 60 days or more) must have a designation on file in the Campus Branch to approve a manual refund. See IRM 3.17.79.3.5, Employees Authorized to Sign Requests for Refunds.
 - b. LTAs approving manual refunds automatically have their Integrated Data Retrieval System (IDRS) profile restricted. See IRM 10.8.34.10.2.1.6.8, Automated Command Code Access Control.
 - c. LTAs must verify employees conducted proper research. This includes, but is not limited to, consideration of statute expiration dates.
 - d. LTAs must ensure the manual refund is within TAS's authorities (see IRM 13.1.4, TAS Authorities) and the circumstances of the case warrant such action. Make an Account Technical Advisor (ATA) referral if you have questions or issues. See IRM 13.1.12.2.2, Requesting Assistance from Technical Advisors.
 - e. Before the LTA approves the manual refund request, they must follow IRM 1.4.13.9.5.4.6, Manual Refund Reviews, to ensure it is properly reviewed.
- (4) In the event an erroneous and duplicate manual refund occurs, LTAs will follow the procedures found in IRM 21.4.5, Erroneous Refunds.
- (5) Area Offices are responsible for conducting Area Analyst MR Reviews and reviews of manual refund processing during Operational Reviews. See IRM 1.4.13.9.6.4.6(5), Manual Refund Reviews.

13.10.2.2.1.1
(09-09-2025)

Manual Refund Training

- (1) TAS employees involved in initiating, reviewing, and signing manual refunds must complete the most recent manual refund training courses available via Integrated Talent Management (ITM) as identified below:

ITM Course Number and Name:	Required for:
Course 30914, Manual Refunds	<p>All employees that initiate, review, and sign manual refunds.</p> <p>Note: An employee can take Course 30914a instead of Course 30914 if the employee completed Course 30914 in the previous year. This substitution does not apply if there is a change to Course 30914 in the current year or if there is a gap between years when the employee took Course 30914 or Course 30914a.</p>

- (2) These employees must complete all training annually within the period of **January 1 to February 1** or **prior to** IDRS Unit Security Representatives (USRs) assigning IDRS command code (CC) RFUND or a manual refund profile restriction (RSTRK (M)).
- (3) These employees must **timely** complete all training. USRs will remove CC RFUND from the IDRS profile of any employee who fails to timely complete the required annual training.
- (4) TAS must maintain and have available for review by internal and external stakeholders, **all** training documentation recorded in ITM.

13.10.2.2.2
(09-09-2025)
Payment Processing

- (1) Generally, TAS does not accept any form of payment from taxpayers. However, if TAS mistakenly receives non-cash remittances, refer to IRM 21.1.7.9.20, Discovered Remittance, and IRM 3.8.46, Discovered Remittance. Guidance on remittance issues changes frequently and an awareness of procedures for remittance allows TAS to accurately and timely assist taxpayers. Keep in mind:
 - a. TAS cannot accept cash payments. Instead, TAS should refer the taxpayer to the local Taxpayer Assistance Center for payment processing. See IRM 21.3.4.7, Remittance Processing, for additional information.
 - b. Procedures are in place to ensure TAS handles non-cash remittances appropriately and timely within one day.
 - c. TAS prepares Form 3244, Payment Posting Voucher, for all remittances.
 - d. TAS uses Form 3210, Document Transmittal, to send payments to the Campus for posting.
 - e. If the Teller observes a critical error, they will inform the manager via e-Trak. See IRM 3.8.47.7.1, Critical Errors.

13.10.2.2.3
(09-09-2025)
Return Processing

- (1) Situations in which TAS employees should accept an unprocessed original or amended return are extremely rare. If TAS receives a return that is time-sensitive (*e.g.*, received on the due date for filing or on the last day a taxpayer can claim a refund), and it is not possible to get the original document to the appropriate campus that same day, then TAS may accept the return for processing. **A hardship alone is not reason to accept an original or amended tax return.** For additional guidance on receiving original returns, refer to IRM 13.1.18.8.3, Taxpayers Delivering Returns to TAS and TAS Date Stamp, and IRM 13.1.24.6.2.7.1, Time Sensitive Unprocessed Original Return Procedures.
- (2) See also IRM 13.1.24.6.2, Advocating for Taxpayers Seeking Offset Bypass Refunds.

13.10.2.2.4
(09-09-2025)
Integrated Data Retrieval System (IDRS)

- (1) IDRS accesses Master File account information using IDRS CCs. Through wide-area networks, IDRS accesses:
 - Corporate Files On-line (CFOL);
 - Files residing at the computing centers; and
 - Taxpayer Information Files (TIF).
- (2) IDRS provides the means to:
 - Take control of and take action on cases. For more information on creating, modifying, and closing IDRS control bases, see IRM

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

13.1.16.8(5) and (6), Sources of TAS Cases and Initial Intake Actions; IRM 13.1.18.5(5), Initial Actions; and IRM 13.1.21.2.1(3), Closing Actions.

- Request and receive printouts of modules.
- Research accounts.
- Research or extract from Master File tapes.

13.10.2.2.4.1 (09-09-2025) IDRS Security

- (1) It is the policy of the IRS to protect its information resources and allow the use, access, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) Circulars, Treasury Directives, National Institute of Standards and Technology Publications, and other regulatory guidance. Employees shall protect all Information Technology (IT) resources the IRS owns or uses at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
- (2) The IDRS Security System provides protection for both taxpayers and the employee using IDRS. TAS must protect taxpayers from:
 - Unauthorized disclosures of account information;
 - Unauthorized changes of account information; and
 - Unauthorized accesses (UNAX) to account information.
- (3) IDRS allows users to sign off the system using the F12 function key, then Page Up or XMIT. IDRS systemically signs off a user with an open IDRS session who is inactive for 120 minutes. A screen message notifies the user that IDRS has signed them off. Users systemically signed off may sign back onto IDRS.
 - a. A user who wants to prevent a systemic sign off may return to IDRS, clear the IDRS screen and press the transmit key to restart the 120-minute countdown.
 - b. A user who expects to be away from their workstation for less than 120 minutes may either sign off IDRS and remove their SMART ID card to lock their computer or remove their SMART ID card to lock their computer.
 - c. A user who expects to be away from their workstation for 120 minutes or more must sign off IDRS and remove their SMART ID card to lock their computer.
 - d. The IDRS security system provides a report with the monthly count of IDRS systemic user sign-offs.
 - e. Managers must advise users with 15 or more systemic sign-offs in one month of the expectation to properly sign off when away from their workstations or not actively using IDRS.
- (4) TAS has Maximum Profile Authorization Files (MPAFs) for position groups that access IDRS. TAS based each MPAF upon CCs consistent with each position group's business needs and delegated authority to research and adjust a taxpayer's account. See IRM 13.1.4, TAS Authorities. The TAS MPAFs are in:
 - Exhibit 13.10.2-1, IDRS MPAF for Case Advocates (Including Lead Case Advocates);
 - Exhibit 13.10.2-2, IDRS MPAF for Intake Advocates (Including Lead Intake Advocates);

- Exhibit 13.10.2-3, IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors;
 - Exhibit 13.10.2-4, IDRS MPAF for Quality Analysts;
 - Exhibit 13.10.2-5, IDRS MPAF for TAS Managers;
 - Exhibit 13.10.2-6, Command Codes for IDRS Online Reviews of Account Adjustments;
 - Exhibit 13.10.2-7, Security Command Codes for Unit Security Representatives; and
 - Exhibit 13.10.2-8, Security Command Codes for Terminal Operators.
- (5) While TAS MPAFs specify which CCs may be granted to a user by profile type and position, USRs should only grant these CCs to a user with the delegated authority to use the CC and when the CC is needed to accomplish the user's official duties. Managers with a business justification may approve temporary deviations from the default MPAFs described in IRM 13.10.2.2.4.1.1, Making Deviations from an IDRS MPAF.
- (6) TAS has defined the following profile types for TAS IDRS users:

Note: A user may have more than one profile type.

Profile Type	Description of Profile Type	TAS Position(s) with a business reason to access IDRS typically assigned to the profile type	TAS MPAF typically assigned to the profile type
Full Access	User has research, sensitive, and adjustment CCs. Adjustment CCs allow the user to make changes to tax credits and entitlements. Employees must have the delegated authority to take the action on IDRS and have a business reason to use the CCs. See IRM 13.1.4, TAS Authorities. User must CMODE out of Andover to the designated IMF and BMF office. The user must have the Null feature set to "On" See Exhibit 13.10.2-9, IDRS Multiple Access Table.	<ul style="list-style-type: none"> • Lead Case Advocates (LCAs); • Lead Intake Advocates (LIAs); • CAs; and • Intake Advocates (IAs). 	<ul style="list-style-type: none"> • Exhibit 13.10.2-1; and • Exhibit 13.10.2-2.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Profile Type	Description of Profile Type	TAS Position(s) with a business reason to access IDRS typically assigned to the profile type	TAS MPAF typically assigned to the profile type
Manager	User has research and USR CCs.	<ul style="list-style-type: none"> • LTA; • Taxpayer Advocate Group Manager (TAGM); and • Other TAS Manager whose employees have access to IDRS. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-5.
Research	User has research CCs and a business reason to research taxpayer accounts. Employees in this group do not have the delegated authority and/or business need for IDRS adjustment codes. TAS will use RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research profile to ensure they do not inadvertently have CCs added .	<ul style="list-style-type: none"> • Secretary; • Management Assistant; • Program Analyst; • Management Program Analyst; • Tax Analyst; • System Analyst; • Case Advocacy Specialists; and • Technical Advisor. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-3.
Research – Quality Review	User has research CCs and a business reason to research taxpayer accounts. Employees in this group are prohibited from having any command codes that could potentially change the outcome of a case review. TAS will use RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research – Quality Review profile to ensure they do not inadvertently have CCs added.	<ul style="list-style-type: none"> • Quality Analyst. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-4.

Profile Type	Description of Profile Type	TAS Position(s) with a business reason to access IDRS typically assigned to the profile type	TAS MPAF typically assigned to the profile type
Reviewer	User has quality review CCs needed to conduct IDRS online reviews of account adjustments. See IRM 1.4.13.9.5.4.16.	<ul style="list-style-type: none"> • LTA; • TAGM; • Centralized Case Intake (CCI) Manager; • LIA; and • LCA. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-6.
USR	User has the CCs needed to complete USR responsibilities. IRM 13.10.2.2.4.2.	<ul style="list-style-type: none"> • Individuals with USR responsibilities. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-7.
Terminal Security Administrator (TSA)	User has the CCs needed to complete terminal security administration.	<ul style="list-style-type: none"> • Individuals with terminal security responsibilities. See IRM 10.8.34.2.2.10. 	<ul style="list-style-type: none"> • Exhibit 13.10.2-8.

- (7) TAS will use RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research Profile Type. For exceptions to the use of RSTRK Definer U for employees with a Research Profile Type, see IRM 13.10.2.2.4.1.1.
- (8) TAS USRs will ensure IDRS profiles of LTAs approving manual refunds are restricted. See IRM 10.8.34-9.
- (9) TAS IDRS units and the multiple accesses authorized for them are as follows:
- Groups 63100, 63110, 63200, 63300, 63400, 63500, 63600, 63700, 63800, 63850, and 63880 are Manager Units and read ANY for all campuses access.
 - Technical Analysis and Guidance (TAG), Executive Director Systemic Advocacy (EDSA), and Internal Technical Advisor Program (ITAP) groups read ANY for all campuses access for 63102, 63111 through 63113, and 63120 through 63125.
 - Any user with CC RFUND in their profile may have access to all Submission Processing Campuses.
 - See Exhibit 13.10.2-9, IDRS Multiple Access Approval Table.

Note: Managers must check new members of their group's profile for any Social Security number restrictions. (If any restrictions exist, managers must not add adjustment CCs to that user's profile.) See IRM 10.8.34, IDRS Security Controls.

Reminder: Managers must address changes to profiles as users change positions, either permanently or on detail.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

13.10.2.2.4.1.1
(09-09-2025)

Making Deviations From an IDRS MPAF and RSTRK Definer U

- (1) Managers with a business justification may approve temporary deviations from the default MPAFs described in IRM 13.10.2.2.4.1 (6). However, managers cannot approve the inclusion of any IDRS CC that is not within the user's delegated authority and Exhibit 13.10.2-1. The manager will track all approved deviations on the IDRS CC Deviation Tracking Sheet and provide a copy to their Deputy Executive Director Case Advocacy (Deputy), Deputy Executive Director Systemic Advocacy (DEDSA), or Director (if Headquarters) monthly.
- (2) Managers with a business justification may approve temporary deviations from the use of RSTRK Definer U for employees with a Research Profile Type (see IRM 13.10.2.2.4.1 (7)). However, managers cannot approve the inclusion of any IDRS CC that is not within the user's delegated authority and Exhibit 13.10.2-1. The manager will track all approved deviations on the *IDRS CC Deviation Tracking Sheet* and provide a copy to their Deputy, DEDSA, or Director (if Headquarters) monthly.
- (3) Managers will review all their approved deviations every 30 days and will remove or have the unit's USR remove the CC(s) from the employee's profile when the CC(s) is no longer needed.
- (4) Each month, the Deputy, DEDSA, Director, or designee will compare the tracking sheet to the appropriate MPAF. The Deputy, DEDSA, or Director will discuss any deviations, concerns, or issues with the manager. This process will also be reviewed during all Operational Reviews.
- (5) Technical Analysis & Guidance (TAG) will issue a reminder email at the beginning of each month to the IDRS Area analyst point of contact (POC) to complete the *IDRS CC Deviation Tracking Sheet*.
- (6) IDRS Area analyst POCs will inform local offices monthly of the deviation tracking sheet due date.
- (7) Local office managers will submit their deviation tracking sheet to their IDRS Area analyst POC.
- (8) Each IDRS Area analyst POC will consolidate their local office deviations and send the listing via email to *TAS IDRS Security by the designated due date.
- (9) TAG will roll up the deviations and retain the master tracking sheet.

13.10.2.2.4.2
(09-09-2025)

Authorized IDRS Access

- (1) Employees are permitted to access only those tax modules required to accomplish your official duties. All actions employees take on IDRS, both authorized and unauthorized, are recorded for an audit trail of the user.
- (2) Form 11377-E, Taxpayer Data Access, is a fillable form that will automatically generate a control number that employees use to document an inadvertent access.
- (3) Employees should complete Form 11377-E by close of business on the day of the inadvertent or questionable access (electronic and paper) and forward the signed copy to their manager to document certain inadvertent or questionable accesses that could include one of the following. See IRM 10.5.5.3.5, Employee UNAX Responsibilities, and *When should I complete Form 11377/ 11377-E, Taxpayer Data Access?* for additional information.

- Accessed electronic or paper tax return information in error (such as accidentally entering an incorrect Taxpayer Identification Number).
 - Accessed electronic or paper tax return or tax information of another IRS employee on an assigned case before recognizing the individual as someone known to the employee. See IRM 13.10.2.2.4.2.1, IDRS Access of an IRS Employee Account, for additional information.
 - Accessed electronic or paper tax return or tax information on an assigned case of an individual or organization before recognizing it as belonging to a person or business with whom the employee has a personal or business relationship.
 - Researched another taxpayer's information because it related to an assigned case.
 - Received requests from management to access taxpayer information on cases not assigned to the employee.
- (4) Employees can report inadvertent access of taxpayer information from any system or source, including paper files, using Form 11377-E.
- (5) To submit a Form 11377-E, employees will:
- Complete the form.
- Note:** Form 11377-E requires only the use of the last four digits of the Taxpayer Identification Number (TIN); this includes the comment section.
- Review the Privacy Act Notification located on page 2 of the form.
 - Sign and date the form.
 - Send the form via secure email (along with any supporting documentation) to their manager no later than the end of the day when the access occurred.
- (6) Upon receipt of a Form 11377-E, managers will:
- Review supporting documentation and properly redact TINs using Adobe Acrobat Pro. See Head of Office Designee (HOD) guide in the *Taxpayer Data Access Library* for instructions on redacting information using Adobe Acrobat Pro.
 - Sign and date the form.
- Note:** The manager's signature and date only acknowledge receipt of the documented access. It does not imply acceptance of the access. The access may still be subject to review and investigation.
- Return the employee's copy to the employee as soon as possible. TAS encourages employees to keep their copy for six years. The employee copy will not contain any taxpayer information.
 - Forward the signed IRS copy to the appropriate point of contact (POC). The *HOD Listing* on the *Taxpayer Data Access Library* lists the POCs.
- (7) Upon receipt of a Form 11377-E, the POC will:
- Upload the IRS copy with any supporting documents within five business days of receipt to the *Taxpayer Data Access Library*.
- Note:** Any POC can upload Forms 11377-E to the library. If the employee needs changes to access, managers or POCs will contact the TAS IDRS Online Reports Services (IORS) point of contact (POC) for assistance.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

13.10.2.2.4.2.1
(09-09-2025)

IDRS Access of an IRS Employee Account

- (1) You may access another IRS employee's account information (including TAS employees) the same as any other taxpayer when:
 - a. An inquiry is received in writing or by telephone or you are assigned the case, and
 - b. You do not know the employee.

Caution: If you know the employee making the account inquiry, you must refer the inquiry/case to your manager. See IRM 13.1.17.2(6), Routing a TAS Case.

- (2) There are special procedures that you must follow to protect yourself and the "taxpayer employee." See IRM 10.5.5.3.4, Employee and Contractor UNAX Responsibilities.
- (3) If you receive an inquiry (telephone or written) or are assigned a case of an IRS employee (including TAS employees), and you do not know the employee, complete the authentication check, and work the inquiry or case following TAS procedures in IRM 13.1.16 or IRM 13.1.18. In addition:

If	Then
You receive an inquiry (telephone or written) of an IRS employee (including TAS employees), you do not know the employee, and there is no open TAS case.	Complete a Form 11377-E, Taxpayer Data Access, for each access.
You receive an inquiry (telephone or written) of an IRS employee (including TAS employees), you do not know the employee, and you are assigned the open TAS case.	Complete a Form 11377-E, Taxpayer Data Access, for the initial access only.
You receive an inquiry (telephone or written) of an IRS employee (including TAS employees), you do not know the employee, and there is an open TAS case, but you are not assigned the case.	Complete a Form 11377-E, Taxpayer Data Access, for each access.

- (4) If you receive an inquiry (telephone or written) or are assigned a case of an IRS employee (including TAS employees), and you do know the employee, refer the inquiry or case to your manager. If you accessed the employee's account on IDRS, complete Form 11377-E to document the access.

13.10.2.2.4.3
(09-09-2025)

IDRS Retention Criteria

- (1) IDRS retains an account as long as activity exists as outlined in IRM 2.9.1.13, IDRS Module Retention Criteria for the TIF.
- (2) After three weeks with no activity, IDRS removes the account.

13.10.2.2.4.4
(09-09-2025)
IDRS Message File

- (1) Use CC MESSG to display the information on the IDRS message file.
- (2) Campus Information System employees use the IDRS message file to alert users to problems with local IDRS files and to share pertinent information.
- (3) The information may pertain only to local systems or to problems experienced by all sites.
- (4) CC MESSG will route the user to their campus. If you want to view another campus, use CC MESSG and the campus location code (*e.g.*, MESSG@08).
- (5) Some campuses use the message file to issue IDRS bulletins or local decisions.
- (6) The file advises users of changes in IDRS letters. It also alerts sites to the volumes of special notices mailed to taxpayers that may cause an increase in taxpayer contacts.
- (7) The file may also show campus IDRS profiles, telephone numbers, and PO Box listings.

13.10.2.2.4.5
(09-09-2025)
Manager Responsibilities

- (1) TAS managers of IDRS users are responsible for day-to-day implementation and administration of IDRS security in their unit/group.
- (2) All TAS managers who have employees with access to IDRS will:
 - a. Review and certify profiles of users with sensitive CC combinations in a timely manner. If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
 - b. Review and certify users only have IDRS CC based upon the user's profile type. See IRM 13.10.2.2.4.1 (6) IRM. If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
 - c. Ensure the use of RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research or Research – Quality Review Profile Type.
 - d. Ensure that user profiles are locked when an employee is on leave, in non-duty status, or when the employee will not require IDRS access for 15 to 60 consecutive calendar days (in this case the profile shall be locked on the first day). If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
 - e. Take prompt action to amend the employee access profile or remove the employee from IDRS if they no longer need access, when an employee changes managers or assignments, or leaves the IRS.
 - f. Encourage employees to use the CC LOKME to lock their profiles when they will not need system access for between three and 45 days. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
 - g. Ensure that primary and alternate USRs and IDRS users complete the required initial and annual refresher training.
 - h. Timely review and certify weekly and monthly IDRS Security Reports and take appropriate actions to correct security violations or weaknesses. If the USR is responsible for this action, the manager will ensure that the USR takes all required actions.
 - i. Ensure that managers/USRs are not in the same IDRS unit as the users they oversee. Manager ensures that USRs have been appointed to cover all IDRS units.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

- j. Ensure that IDRS users who meet the criteria for restricted profile types have the appropriate restrictions added to their profiles. In addition, ensure that IDRS users who no longer have restricted roles have the restrictions removed from their profiles. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
- k. Ensure IDRS users utilize the Password Management Capability. If the USR is responsible for this action, the manager ensures that the USR takes all required actions.
- l. Advise users with 15 or more systemic sign-offs for the month of the need to properly sign off when away from their workstations. See IRM 13.10.2.2.4.1 (3).
- m. Reinforce IDRS security through discussions at group meetings.
- n. Periodically verify the accuracy and completeness of the IDRS Unit and USR Database for their office using the *IDRS Unit & USR Database (IUUD)*.
- o. Upon receipt of Form 11377-E, Taxpayer Data Access, sign and date the form, return a copy to the employee, and send to the HOD along with any supporting documents. Within five business days of receipt, the HOD POC must upload the documents to the Taxpayer Data Access Library. See IRM 13.10.2.2.4.1, IDRS Security, for detailed procedures for Form 11377-E.

- (3) Managers are responsible for the activities outlined in IRM 10.8.34.7.1.3, Manager.

13.10.2.2.4.6
(09-09-2025)

Reviewers of IDRS Adjustments

- (1) IDRS Adjustment reviews ensure the integrity and accuracy of adjustments made to taxpayer accounts. This section deals with performing quality reviews of the following IDRS transactions: ADJ54, DRT24, DRT48, FRM34, FRM77 (except Transaction Codes (TCs) 053, 136, 137, 122, 126, and 971 (Action Code 517 only)), CHK64, BNCHG, INCHG, CHKCL, and LPAGE (except inputs without a TIN).
- (2) Reviewers will review 100 percent of online transactions input by new employees during On-the-Job Instruction (OJI). For all other employees, 100 percent review of the online transactions ADJ54/REQ54 and credit transfers (ADD34/FR34, ADD48/DRT48, ADD24/DRT24). All other online transactions may be reviewed as management in the local office deem appropriate.
- (3) Typically, Local Taxpayer Advocates (LTAs), Taxpayer Advocate Group Managers (TAGMs), and Centralized Case Intake (CCI) Managers conduct reviews of IDRS Adjustments. They may delegate these reviews to Lead Intake Advocates (LIAs) and Lead Case Advocates (LCAs). An employee may not conduct a review of their own cases. If a manager delegates the review, the employee conducting the review briefs the manager and the employee involved.
- (4) Reviews will use the IDRS command codes in Exhibit 13.10.2-6 to review online adjustments. See IRM 2.4.5, Command Codes QRADD, QRADD0, QRNCH, QRNCHG, RVIEW, QRACN, and QRIND for the Quality Review System, for procedures for conducting reviews. Contact the IORS POC with questions or concerns.
- (5) When USRs create or reactivate a new IDRS unit, they must ask IDRS User Support at the following Campuses to add their IDRS unit numbers to the EOD 02 data file. Adding the IDRS unit numbers to EOD 02 data file instructs IDRS

at each campus to automatically suspend transactions two days for review ("auto-select"), alleviating the daily input of CC QRADD for each of these campuses.

- Kansas City Campus (KCSC);
- Atlanta Campus (ATSC);
- Cincinnati Campus (CSC);
- Memphis Campus (MSC); and
- Philadelphia Campus (PSC).

- (6) For transactions input over the weekend, use CC QRADD to enter the employee numbers of the employees you plan to review. Suspend all transactions input by your employee or group using CC QRADD or CC QRADDG for the same day. Transactions remain suspended for review for two days. After two days, the system releases all transactions not reviewed for processing to the Master File.
- (7) Use CC QRIND with CC RVIEW to control workloads. CC QRIND requests a summary of a user's transactions available for review for a specific day. Evaluate adherence to IDRS security and procedures.
- (8) Use CC RVIEW to review all transactions or selected transactions input by individual users. Input CC RVIEW within two days after a CC QRADD or a CC QRADDG request to review an adjustment.
- (9) Use CC QRACN to accept, reject, or review your employee's transaction input screens displayed by using CC RVIEW. Review the displayed transaction for quality and appropriate documentation requirements before using CC QRACN.
 - a. Accepted transactions release to the Master Files for processing after the standard two-day hold.
 - b. Rejected transactions change from IDRS status "AP" to "DQ" for following workday. The reviewer must print the action after rejecting the transaction. Send these prints back to the employee for corrective action.
- (10) See IRM 1.4.13.9.5.4.16, IDRS Online Reviews, for the focus of the review.

13.10.2.2.4.7 (09-09-2025) Unit Security Representative Responsibilities

- (1) The USR is an individual who implements and administers IDRS security at the IDRS unit level. TAS will appoint primary USRs in accordance with IRM 10.8.34.7.2.8, Unit Security Representative (USR).
- (2) TAS shall appoint alternate USRs in accordance with IRM 10.8.34.7.2.9, Alternate USR, to assist and/or perform the duties of the primary USR when that individual is not available.
- (3) TAS may appoint temporary USRs and alternate USRs for employees on detail assignments not less than 120 days in accordance with IRM 10.8.34.7.2.8 and IRM 10.8.34.7.2.9.
- (4) TAS USRs are responsible for:
 - a. Reviewing IORS reports for their IDRS unit in accordance with IRM 10.8.34.7.2.11.1, IORS Primary Report Reviewer; IRM 10.8.34.10.3.1.1, IDRS Online Reports Services (IORS); and IRM 10.8.34.10.3.1.2, Review and Certification of Security Reports in IORS.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

- b. Ensuring new and returning users in their IDRS units receive an IDRS security awareness briefing prior to accessing IDRS. See IRM 10.8.34.9.1.1.1, IDRS User Security Awareness Training.
- c. Ensuring users in their IDRS units receive periodic (at a minimum annual) IDRS security awareness briefings. See IRM 10.8.34.9.1.1.1.
- d. Ensuring managers of their IDRS units are fully aware of their IDRS security responsibilities as outlined in IRM 10.8.34.7.1.3.
- e. Completing the required initial and annual refresher training. See IRM 10.8.34.9.1.2.5, Unit Security Representative (USR) and Alternate USR Training.
- f. Monitoring the command code usage of employees with sensitive command code combinations in their profiles. See IRM 10.8.34.10.2.1.6.6, Sensitive Command Codes and Sensitive Command Code Combinations.
- g. Restricting IDRS profiles of LTAs approving manual refunds. See IRM 10.8.34.10.2.
- h. Using RSTRK Definer U (see IRM 10.8.34-11) to restrict employees with a Research or Research – Quality Review IDRS Profile Type. See IRM 13.10.2.2.4.1 (6).

13.10.2.2.4.8

(09-09-2025)

Terminal Security Administrator (TSA)

- (1) The TSA is an individual assigned by TAS to unlock IDRS terminals and unlock employee profiles locked due to 17 consecutive days of inactivity.
- (2) The intent of the TSA role is to reduce USR workload.
- (3) TSAs may either be a non-bargaining unit (NBU) or bargaining unit (BU) employee.
- (4) A TAS Deputy or Director will approve a TSA designation. TAS will submit the IDRS Security TAS POC to the IDRS Security Account Administration staff on Form 13230, IDRS Security Personnel Designation Form. Before submission, the IDRS Security TAS POC will notify the unit's primary USR of the TSA designation so that the USR is aware of who is receiving security command codes.
- (5) The TSA's manager shall submit a Business Entitlement Access Request System (BEARS) modify user request to the IDRS Security Account Administrator to have the appropriate security command codes added to the TSA's IDRS employee profile. See Exhibit 13.10.2-8, Security Command Codes for Terminal Security Administrators. The TSA's primary USR must approve the BEARS modify user request.
- (6) The primary USR must instruct the TSA on the duties of this position.
- (7) Enterprise Operations (EOPS) will review the BEARS request and place CC SECOP in the TSA's profile if approved. SECOP is used to unlock IDRS terminals. At the request of the manager, TSAs may also receive CC UNLEM. TSAs use UNLEM to unlock an employee profile that the system locked because the user was inactive for 17 days.
- (8) USRs are authorized to provide a copy of the "Master Register of Active Users" report or a CC SFINQA screen print to the TSA that lists the IDRS employee numbers of users in their unit(s) when a TSA is given the capability to unlock employee profiles. TSAs are only authorized to unlock IDRS profiles for known users.

- (9) For IDRS security purposes, the TSA's security activity is under the purview of the designated primary USR(s) for that unit or area. If the primary USR has concerns regarding the security actions taken by the TSA, the primary USR may request an IDRS Security Analyst provide an audit trail extract of the TSA activities for a designated date or date range.

13.10.2.2.4.9

(09-09-2025)

TAS IORS POC Responsibilities

- (1) The TAS IORS POC ensures TAS effectively performs IDRS security administration and monitoring. The TAS IORS POC shall:
 - a. Coordinate TAS's response to IORS security report certification related issues.
 - b. Work with USRs and Managers to ensure compliance with the review and certification of IORS reports.
 - c. Participate in Operational Reviews to train Area Analysts on how to conduct a review of IDRS security. See IRM 1.4.13.9.5.3, Operational Reviews.
 - d. Perform quarterly testing of compliance with the TAS MPAF restrictions on IDRS users based on Profile Types. See IRM 13.10.2.2.4.1, IDRS Security.
 - e. Represent TAS at IDRS Security related stakeholder meetings.
 - f. Conduct an annual review of the TAS MPAFs to ensure CCs are consistent with business needs. Find TAS MPAFs at Exhibit 13.10.2-1, Exhibit 13.10.2-2, Exhibit 13.10.2-3, Exhibit 13.10.2-4, Exhibit 13.10.2-5, Exhibit 13.10.2-6, Exhibit 13.10.2-7 and Exhibit 13.10.2-8.
 - g. Obtain the approval of the Executive Director Case Advocacy (EDCA) prior to making any changes to the MPAF.
 - h. Conduct routine testing of IDRS adjustment reviews to ensure reviews are completed as intended. See IRM 1.4.13.9.5.4.16, IDRS Online Reviews.
 - i. Identify training needs for TAS IDRS users, managers, USRs, reviewers of IDRS adjustments, and TSAs.
 - j. Prepare and implement the annual IDRS training plan to ensure users, managers, reviewers of IDRS adjustments, TSAs, and USRs complete initial and annual refresher training (as required).
 - k. Serve as the TAS POC for questions concerning the use and processing of Form 11377-E. See IRM 10.5.5.3.5, Employee UNAX Responsibilities.
- (2) See IRM 10.8.34.7.2.5, IDRS Security Account Administrator, and IRM 10.8.34.10.3.1, IDRS Security Reports, for additional information.

13.10.2.2.4.10

(09-09-2025)

TAS IDRS Business Unit POC Responsibilities

- (1) The TAS IDRS Business Unit POC ensures TAS effectively performs IDRS security administration and monitoring. The TAS IORS POC shall:
 - a. Serve as the TAS POC with the IDRS Security Program Management Office.
 - b. Serve as a liaison between the IDRS Security Program Management Office and TAS in addressing IDRS security issues.
 - c. Coordinate TAS's response to IDRS security related issues.
 - d. Represent TAS at IDRS Security related stakeholder meetings.
 - e. Work with TAS managers and the TAS IORS POC to identify trends or potential IDRS misuse. See IRM 10.8.34.10.3.2, Audit Trails.
- (2) See IRM 10.8.34.7.2.2, IDRS Security Business Division Point-of-Contact, for additional information.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

13.10.2.2.5
(09-09-2025)

TAS Systems Access

- (1) Managers are responsible for ensuring TAS provides employees with systems access to meet business needs, ensuring employees follow the rules pertaining to the use of systems, and timely notifying the system administrators when access is no longer needed. The following tools are available for assistance:
 - a. IRM 10.8.1, Policy and Guidance;
 - b. IRM 10.8.2, IT Security Roles and Responsibilities;
 - c. *Advocacy Tools*; and
 - d. *TAS Technology Hub*.
- (2) Managers must ensure that employees have access to IRS internal or external computer systems containing taxpayer information only necessary to complete their IRS officially assigned duties. See IRM 10.5.5.3.2, Manager UNAX Responsibilities.
- (3) Employees should complete Form 11377, Taxpayer Data Access, or Form 11377-E by close of business on the day of the access and forward the signed copy to their manager to document certain inadvertent accesses. See IRM 10.5.5.3.5, Employee UNAX Responsibilities.

13.10.2.2.5.1
(09-09-2025)

Reserved

- (1) This previous section is removed due to TAMIS change to Phoenix and will be updated after Phoenix goes live.

13.10.2.2.5.2
(09-09-2025)

Reserved

- (1) This previous section is removed due to SAMS change to Phoenix and will be updated after Phoenix goes live.

13.10.2.2.6
(09-09-2025)

Clean Desk Policy

- (1) TAS managers will conduct a review to ensure employees are following the Clean Desk Policy. See IRM 13.10.2.2.6, Clean Desk Policy, for information on how to conduct a review.
- (2) Managers will conduct the reviews at least once a year.
- (3) Managers will conduct clean desk reviews on all TAS employees, including those not directly reporting to them but co-located in their office space.
- (4) Managers will document the completion of the review in a memo format and make the memo available to their immediate supervisor upon request. For co-located employees, the LTA (or other TAS manager) will document the completion of the review in a memo format for each employee and send the memo via secure email to the manager of the employee, when applicable.

13.10.2.2.7
(09-09-2025)

Confidentiality of Tax Returns and Tax Return Information

- (1) All TAS managers must take an active role to prevent willful and attempted unauthorized access and inspection of taxpayer information in electronic and paper form. This involves overseeing employees' work as well as continually stressing the importance of protecting and securing taxpayer records.
- (2) Document 11500, IRS Manager's Guide to Penalty Determinations, states managers may be subject to written reprimand, suspension, or removal for failure to adequately instruct, train, or supervise employees in their responsibilities for record and information protection.
- (3) All managers must:

- a. Communicate with employees on a regular basis to ensure they are aware of UNAX prohibitions and penalties. Frequent communication also ensures employees know how to document and report inadvertent or unintentional access.
- b. Be responsible for the timely and thorough review of available system security reports.
- c. Report suspected UNAX violations or any unusual activity to the Treasury Inspector General for Tax Administration (TIGTA) for investigation.
- d. Monitor and ensure employees have access to IRS internal or external computer systems containing taxpayer information only when necessary to complete their IRS officially assigned duties.
- e. Ensure employees under investigation by TIGTA for UNAX violations are promptly removed from IDRS and any other IRS computer system requiring administrative approval and containing taxpayer information. Managers must also remove these employees from other tax-related duties.
- f. Ensure Form 11377, or Form 11377-E, Taxpayer Data Access, are forwarded to the head of office designee. Form 11377 or Form 11377-E documents accesses to taxpayer information not supported by direct case assignment or which may otherwise appear questionable. A manager's signature on this form does not imply authorization for documented accesses. The access may still be subjected to further review and investigation.
- g. Make timely reassignments whenever an employee reports having a covered relationship with an individual or organization in an assigned tax duty which may cause a conflict of interest. An employee can use Form 4442, Inquiry Referral, to request such reassignments and avoid a possible conflict of interest.
- h. Educate employees to avoid UNAX violations and ensure employees know the potential consequences of their actions.
- i. Lead by example.
- j. Control employees' access to IRS internal or external computer systems via the BEARS approval process, granting access only when required to complete official duties and removing it when no longer required to complete official duties.
- k. Always refer questionable accesses to TIGTA. See *U.S. Treasury Inspector General for Tax Administration*.

13.10.2.2.8
(09-09-2025)
Disclosure

- (1) IRM 11.3, Disclosure of Official Information, provides the instructions, guidelines, and procedures necessary for managers to fulfill their obligations under the disclosure laws.
- (2) The *Disclosure and Privacy Knowledge Base* has many tools available to assist TAS employees and managers in understanding and applying their disclosure responsibilities.
- (3) Additional resources:
 - a. *What is considered PII?*
 - b. IRM 10.5.4, Incident Management Program;
 - c. *Cyber Security*;
 - d. Managers must report incidents involving intentional unauthorized disclosures to *TIGTA*;

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

- e. IRM 11.3.38.5.1, Reporting Non-willful Inadvertent Disclosures of Sensitive Information, and IRM 11.3.38.5, Reporting of Suspected Willful Unauthorized Accesses or Disclosures.
- f. IRM 13.1.10.13.3, Handling a FOIA Request.

13.10.2.2.9
(09-09-2025)

Records Retention

- (1) The life-cycle of records begins when an employee either creates or receives a record and usually ends when the employee destroys the record or transfers it to the National Archives and Records Administration (NARA). See IRM 1.15, The Records and Information Management Program, for detailed information on the types of records and their life-cycles. Each TAS employee must:
 - a. Manage the records they create and/or maintain in accordance with policies outlined in Document 12990, Records Control Schedules (p. 33-47) for records pertaining to TAS), and Document 12829, General Records Schedules;
 - b. Assure the integrity and confidentiality of the records in their custody that they use to do their jobs. Managers are responsible for ensuring that their employees comply with these requirements; and
 - c. Return records requested from the Federal Records Center (FRC) promptly when finished with the records.
- (2) The Records Control Schedules cover all aspects of TAS's records, including (but not limited to) General Administrative Records; records pertaining to the Annual Reports to Congress; National Taxpayer Advocate Speech Files, Testimonies, and Public Appearances; Form 911, Application for Taxpayer Assistance Order (ATAO); case files; LITC grant files, Advocacy Project Reports, etc. For a full listing, see Document 12990.
- (3) For additional resources, see IRM 1.15.6, Managing Electronic Records.
- (4) For information concerning litigation holds, see IRM 13.1.5.9, Disclosure to Counsel, DOJ, or the U.S. Attorney's Office, and IRM 13.1.10.2.6, Requests for TAS Employees to Testify or Produce IRS Records or Information.

13.10.2.2.10
(09-09-2025)

Financial Guidelines

- (1) IRM 1.33.4, Financial Operating Guidelines, assists Financial Plan Managers (FPMs) and other budget and finance professionals in fulfilling their responsibilities to effectively manage budgetary resources.
- (2) This guidance focuses on managing, monitoring, and controlling the money Congress appropriates to the IRS, including user fees. In compliance with the **Antideficiency Act** and applicable provisions of appropriations law, the IRS cannot spend or obligate more than Congress has appropriated and may use funds only for purposes specified in law. Additionally, the **Antideficiency Act** prohibits the IRS from spending or obligating funds in advance of an appropriation, unless the law has provided specific authority to do so. Every Operating Division has an FPM who must comply with the **Antideficiency Act** and appropriations law.

13.10.2.2.11
(09-09-2025)

TAS Space Requirements

- (1) *The National Workspace Standards* provide guidance for Facilities Management & Security Services (FMSS) during facilities planning and space allocation in new construction, renovation, rent reduction, and relocation projects. The standards reflect the need for TAS independence by requiring a stand-alone (enclosed) suite for TAS.

- a. TAS offices will have an interview room, a reception area and a Conference Room. Interview rooms and reception areas should have entrances from outside of the work area. A taxpayer should not need to enter the work area to get to either the interview room or reception area.
 - b. Interview rooms must have duress alarms.
 - c. Interview rooms and conference rooms should be adjacent to the reception area.
 - d. Due to TAS independence requirements, TAS employees must maintain a space separate from all IRS functions. This space should typically be an enclosed space walled off from other IRS functions.
- (2) To the extent possible, TAS will provide employees with standard sized workstations in compliance with the *2022 National Agreement*, Article 11.
 - (3) To the extent possible, TAS will provide its Managers and Executives appropriate offices within the TAS space.
 - (4) Any deviation from the established seating and space requirements must be due to extenuating circumstances and require TAS Executive approval.

13.10.2.2.11.1
(09-09-2025)

**Local Point of Contact
(LPOC) Responsibilities**

- (1) Once a space project is approved and funded, FMSS contacts Finance and Human Capital (FHC) to request the name of a local point of contact (LPOC) who will represent TAS for the duration of the project. This LPOC will work with the space coordinator in FHC during the project. The LPOC is typically the LTA on site but can be any NBU TAS employee.
- (2) The role of the LPOC is to represent TAS during the design and implementation of the project. This includes keeping remote TAS managers informed of issues that may impact their employees located at the project site. The LPOC should elevate any issues they cannot resolve with the FMSS project manager to the space coordinator in FHC. TAS FHC must review and approve final floor plans prior to finalizing any space change with FMSS. Please email *TAS Space any time you are contacted by FMSS regarding a change to space you are responsible for to ensure FHC provides the support and guidance you need throughout the process.

This Page Intentionally Left Blank

Exhibit 13.10.2-1 (09-09-2025)
IDRS MPAF for Case Advocates (Including Lead Case Advocates)

ACTON	ADC24	ADC34	ADC48	ADD24	ADD34
ADD48	ADJ54	ADOPT	AMDIS	ATINQ	BMFOL
BMFOR	BNCHG	BRTVU	CDPTR	CFINK	CHK64
CHKCL	COMPA	DDBCVC	DDBKD	DDBOL	DDPOL
DFAST	DLITE	DM1DT	DOALL	DRT24	DRT48
DTVUE	DUPED	DUPOL	EFTAD	EFTPS	EICMP
EICPV	ELFRQ	EMFOL	ENMOD	ENREQ	EOGEN
ERINV	ERTVU	ERUTL	ESTAB	FINDE	FINDS
FFINQ	FIEMP	FRM34	FRM49	FRM77	FTBOL
FTDPN	IADIS	IAGRE	IAORG	IAPND	IAREV
ICOMP	IMFOB	IMFOL	IMFOR	INCHG	INOLE
INTST	IRCHG	IRPOL	IRPTR	ISTSR	LETER
LEVYS	LOCAT	LPAGE	LPAGD	MFREQ	MFTRA
NAMEB	NAMEE	NAMEI	NAMES	NOREF	P8453
PATRA	PICRD	PIEST	PIFTD	PIFTF	PINEX
PMFOL	R8453	RECON	REINF	REQ54	REQ77
RFINK	RFUND	RPINK	RPVUE	RTFTP	RTVUE
SCFTR	STATB	STATI	STAUP	SUMRY	TDINQ
TELEA	TELEC	TELED	TELER	TERUP	TPCIN
TPCOL	TPIIP	TRDBV	TRDPG	TRPRT	TSUMY
TXCMP	TXMOD	UNLCE	UPCAS	UPDIS	UPRES
UPTIN	URINQ	VPARS	XSINQ		

Revision History for CC:

- Added DFAST on 1/22/2013;
- Added EOGEN on 4/1/2013;
- Added IRPOL on 3/15/2016;
- Added DLITE on 6/11/2018;
- Added TRDPG on 7/27/2019;
- On 2/23/2022, changed the MPAF from applying to all TAS IDRS users to applying to only Case Advocates and created new MPAFs for all other positions. Removed the following CC as a result of an IDRS Risk Assessment: ASGNB, ASGNI, EFTNT, IADFL, LEVYD, LEVYE, LEVYM, LEVYR, TDIRQ, and TSIGN; and
- Removed EFTOF on 9/7/2023. TAS employees do not have the delegated authority to input skip payments on Direct Debit Installment Agreements (DDIAs); therefore, TAS has removed it since employees use this CC solely to input skip payments for DDIAs.

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-2 (09-09-2025)

IDRS MPAF for Intake Advocates (Including Lead Intake Advocates)

ACTON	ADJ54	ADOPT	AMDIS	ATINQ	BMFOL
BMFOR	BNCHG	BRTVU	CDPTR	CFINK	CHK64
CHKCL	DDBCVC	DDBKD	DDBOL	DDPOL	DFAST
DLITE	DOALL	DTVUE	DUPOL	EFTAD	EFTPS
EICMP	EICPV	ELFRQ	EMFOL	ENMOD	ENREQ
EOGEN	ERINV	ERTVU	ERUTL	ESTAB	FINDE
FINDS	FFINQ	FIEMP	FTBOL	IADIS	IAGRE
IAORG	IAPND	IAREV	ICOMP	IMFOB	IMFOL
IMFOR	INCHG	INOLE	INTST	IRCHG	IRPOL
IRPTR	ISTSR	LETER	LEVYS	LOCAT	LPAGD
LPAGE	MFREQ	MFTRA	NAMEB	NAMEE	NAMEI
NAMES	P8453	PATRA	PICRD	PIEST	PIFTD
PIFTF	PINEX	PMFOL	R8453	RECON	REINF
REQ54	RFINK	RPINK	RPVUE	RTFTP	RTVUE
SCFTR	STATB	STATI	STAUP	SUMRY	TDINQ
TELER	TERUP	TPCIN	TPCOL	TPIIP	TRDBV
TRDPG	TRPRT	TSUMY	TXCMP	TXMOD	UNLCE
UPCAS	UPDIS	UPTIN	URINQ	VPARS	XSINQ

Exhibit 13.10.2-3 (09-09-2025)

IDRS MPAF for Secretaries, Management Assistants, Program Analysts, Management Program Analysts, Tax Analysts, Systems Analysts, Case Advocacy Specialists, and Technical Advisors

ACTON	ADOPT	AMDIS	ATINQ	BMFOL	BMFOR
BRTVU	CDPTR	CFINK	COMPA	DDBCX	DDBKD
DDBOL	DDPOL	DFAST	DLITE	DOALL	DTVUE
DUPOL	EFTAD	EFTPS	EICMP	EICPV	ELFRQ
EMFOL	ENMOD	EOGEN	ERINV	ERTVU	ERUTL
ESTAB	FINDE	FINDS	FFINQ	FIEMP	FTBOL
FTDPN	IADIS	ICOMP	IMFOB	IMFOL	IMFOR
INOLE	INTST	IRPOL	IRPTR	ISTSR	LETER
LEVYS	LOCAT	LPAGE	LPAGD	MFREQ	MFTRA
NAMEB	NAMEE	NAMEI	NAMES	P8453	PATRA
PICRD	PIEST	PIFTD	PIFTF	PINEX	PMFOL
R8453	RECON	REINF	RFINK	RPINK	RPVUE
RTFTP	RTVUE	SCFTR	SUMRY	TDINQ	TELER
TPCIN	TPCOL	TPIIP	TRDBV	TRDPG	TRPRT
TSUMY	TXCMP	TXMOD	UNLCE	UPCAS	UPDIS
UPTIN	URINQ	VPARS	XSINQ		

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-4 (09-09-2025)

IDRS MPAF for Quality Analysts

ACTON	ADOPT	AMDIS	ATINQ	BMFOL	BMFOR
BRTVU	CDPTR	CFINK	COMPA	DDBCVC	DDBKD
DDBOL	DDPOL	DFAST	DLITE	DTVUE	DUPOL
EFTAD	EFTPS	EICMP	EICPV	ELFRQ	EMFOL
ENMOD	EOGEN	ERINV	ERTVU	ERUTL	ESTAB
FINDE	FINDS	FFINQ	FIEMP	FTBOL	FTDPN
IADIS	ICOMP	IMFOL	IMFOR	INOLE	INTST
IRPOL	IRPTR	ISTSR	LEVYS	LOCAT	MFTRA
NAMEB	NAMEE	NAMEI	NAMES	P8453	PATRA
PICRD	PIEST	PIFTD	PIFTF	PINEX	PMFOL
R8453	REINF	RFINK	RPINK	RPVUE	RTFTP
RTVUE	SCFTR	SUMRY	TDINQ	TPIIP	TRDBV
TRDPG	TRPRT	TSUMY	TXCMP	TXMOD	UPTIN
URINQ	XSINQ				

Exhibit 13.10.2-5 (09-09-2025)
IDRS MPAF for TAS Managers

ACTON	ADOPT	AMDIS	ATINQ	BMFOL	BMFOR
BRTVU	CDPTR	CFINK	COMPA	DDBCVC	DDBKD
DDBOL	DDPOL	DFAST	DLITE	DOALL	DTVUE
DUPOL	EFTAD	EFTPS	EICMP	EICPV	EMFOL
ENMOD	EOGEN	ERINV	ERTVU	ERUTL	ESTAB
FINDE	FINDS	FFINQ	FIEMP	FTBOL	FTDPN
IADIS	ICOMP	IMFOB	IMFOL	IMFOR	INOLE
INTST	IRPOL	IRPTR	ISTSR	LETER	LEVYS
LOCAT	LPAGE	LPAGD	MFREQ	MFTRA	NAMEB
NAMEE	NAMEI	NAMES	P8453	PATRA	PICRD
PIEST	PIFTD	PIFTF	PINEX	PMFOL	R8453
RECON	REINF	RFINK	RPINK	RPVUE	RTFTP
RTVUE	SCFTR	STAUP	STATB	STATI	SUMRY
TDINQ	TELER	TPCIN	TPCOL	TPIIP	TRDBV
TRDPG	TRPRT	TSUMY	TXCMP	TXMOD	UNLCE
UPCAS	UPDIS	UPTIN	URINQ	VPARS	XSINQ

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-6 (09-09-2025)

Command Codes for IDRS Online Reviews of Account Adjustments

QRACN	QRADD	QRIND	QRNCH	RVIEW
-------	-------	-------	-------	-------

Exhibit 13.10.2-7 (09-09-2025)
Security Command Codes for Unit Security Representatives

MRINQ	REPTS	RSTRK	SECOP	SFINQ	UPEMP
UPTRM					

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-8 (09-09-2025)

Security Command Codes for Terminal Security Administrators

SECOP	UNLEM
-------	-------

Exhibit 13.10.2-9 (09-09-2025)
IDRS Multiple Access Approval Table

TAS employees with adjustment CCs, including CC STAUP, are required to CMODE out of Andover to the designated IMF and BMF office. The user must have the Null feature set to "On." See IRM 13.10.2.2.4.1 (6) .

TAS Function	IDRS Unit Number	Multiple Access	Campus for Manual Refunds
TAS USRs	63110	Any	N/A
TAS IORS POC and TAS IDRS POC	63487	Any	N/A
1 - Deputy	63100	Any	N/A
1 - Albany	63165	BR and FR	AU, KC, and OG
1 - Andover	63850, 63861, 63862, 63863	KC and PH	AU, KC, and OG
1 - Augusta	63851	KC and PH	AU, KC, and OG
1 - Boston	63856	KC and PH	AU, KC, and OG
1 - Brookhaven	63131-63134	BR, CI, and FR	AU, KC, and OG
1 - Brooklyn	63170	BR, CI, and FR	AU, KC, and OG
1 - Buffalo	63181	CI and FR	AU, KC, and OG
1 - Burlington	63855	KC and PH	AU, KC, and OG
1 - Hartford	63859	KC and PH	AU, KC, and OG
1 - Manhattan	63190-63191	BR and FR	AU, KC, and OG
1 - Portsmouth	63854	KC and PH	AU, KC, and OG
1 - Providence	63857	KC and PH	AU, KC, and OG
1 - Reserved	63880	N/A	N/A
2 - Deputy	63200	Any	N/A
2 - Baltimore	63231-63232	AT, OG, and PH	AU, KC, and OG
2 - Charlotte	63258-63259	OG and PH	AU, KC, and OG
2 - DC LTA	63101	AT and PH	AU, KC, and OG
2 - Greensboro	63211-63212	AT and PH	AU, KC, and OG
2 - Newark DE	63270	AT, CI, OG, and PH	AU, KC, and OG
2 - Philadelphia	63252-63254	OG and PH	AU, KC, and OG
2 - Pittsburgh	63260-63261	AT, OG, and PH	AU, KC, and OG
2 - Richmond	63220	AT and PH	AU, KC, and OG
2 - Springfield NJ	63140	AT, CI, and PH	AU, KC, and OG

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-9 (Cont. 1) (09-09-2025)
IDRS Multiple Access Approval Table

TAS Function	IDRS Unit Number	Multiple Access	Campus for Manual Refunds
2 - Trenton NJ	63241	AT, CI, and PH	AU, KC, and OG
3 - Deputy	63300	Any	N/A
3 - Atlanta City Center	63301-63304	AU, CI, and ME	AU, KC, and OG
3 - Birmingham	63311, 63331	AU and ME	AU, KC, and OG
3 - Clearwater	63373, 63391	AU, AT, CI, and ME	AU, KC, and OG
3 - Columbia SC	63201	AT and PH	AU, KC, and OG
3 - Jacksonville	63330-63334	AU, CI, and ME	AU, KC, and OG
3 - Ft. Lauderdale	63371-63372	AU, AT, CI, and ME	AU, KC, and OG
3 - Puerto Rico	63171-63173	OG and PH	AU, KC, and OG
4 - Deputy	63400	Any	N/A
4 - Cincinnati	63440, 63442, 63443	CI and KC	AU, KC, and OG
4 - Cleveland	63450 - 63452	CI and KC	AU, KC, and OG
4 - Covington	63343	CI and KC	AU, KC, and OG
4 - Detroit	63410-63420	CI and KC	AU, KC, and OG
4 - Indianapolis	63461-63463	CI and KC	AU, KC, and OG
4 - Louisville	63470	CI and KC	AU, KC, and OG
4 - Memphis	63482-63483	KC and ME	AU, KC, and OG
4 - Nashville	63490-63491	CI and KC	AU, KC, and OG
4 - West Virginia	63480	CI and KC	AU, KC, and OG
5 - Deputy	63500	Any	N/A
5 - Austin	63511, 63514, 63518	AU and ME	AU, KC, and OG
5 - Dallas	63520-63524	AU and ME	AU, KC, and OG
5 - El Paso	63510	FR and OG	AU, KC, and OG
5 - Houston	63501, 63503, 63504	AU and ME	AU, KC, and OG
5 - Jackson	63321	AU and ME	AU, KC, and OG
5 - Little Rock	63350	AU and ME	AU, KC, and OG
5 - New Orleans	63355-63356	AU, CI, and ME	AU, KC, and OG
5 - Oklahoma City	63531	FR and OG	AU, KC, and OG
6 - Deputy	63600	Any	N/A

Exhibit 13.10.2-9 (Cont. 2) (09-09-2025)
IDRS Multiple Access Approval Table

TAS Function	IDRS Unit Number	Multiple Access	Campus for Manual Refunds
6 - Chicago	63806-63807	KC and ME	AU, KC, and OG
6 - Des Moines	63826	AU and ME	AU, KC, and OG
6 - Fargo	63648	FR and OG	AU, KC, and OG
6 - Kansas City	63803-63805	KC and ME	AU, KC, and OG
6 - Milwaukee	63809	CI and KC	AU, KC, and OG
6 - Sioux Falls	63655	FR and OG	AU, KC, and OG
6 - Springfield, IL	63808	CI and KC	AU, KC, and OG
6 - St. Louis	63828-63829	AU and ME	AU, KC, and OG
6 - St. Paul	63810	AU and ME	AU, KC, and OG
6 - Wichita	63831	FR and OG	AU, KC, and OG
7 - Deputy	63700	Any	N/A
7 - Albuquerque	63507	FR and OG	AU, KC, and OG
7 - Boise	63630	FR and OG	AU, KC, and OG
7 - Cheyenne	63610	FR and OG	AU, KC, and OG
7 - Denver	63540-63542	FR and OG	AU, KC, and OG
7 - Helena	63640	FR and OG	AU, KC, and OG
7 - Las Vegas	63775	FR and OG	AU, KC, and OG
7 - Ogden	63691-63694	FR and OG	AU, KC, and OG
7 - Omaha	63830	AU and OG	AU, KC, and OG
7 - Phoenix	63560-63561	FR and OG	AU, KC, and OG
7 - Reserved	63601	N/A	N/A
7 - Reserved	63660	N/A	N/A
8 - Deputy	63800	Any	N/A
8 - Anchorage	63795	FR and OG	AU, KC, and OG
8 - Fresno (LTA)	63751-63753	FR and OG	AU, KC, and OG
8 - Honolulu	63750	FR and OG	AU, KC, and OG
8 - Laguna Niguel	63741-63742	FR and OG	AU, KC, and OG
8 - Los Angeles	63702 -63704	FR and OG	AU, KC, and OG
8 - Oakland	63711, 63712	FR and OG	AU, KC, and OG
8 - Portland	63670	FR and OG	AU, KC, and OG

13.10 Taxpayer Advocate Service (TAS) Policies, Procedures and Internal Controls

Exhibit 13.10.2-9 (Cont. 3) (09-09-2025)

IDRS Multiple Access Approval Table

TAS Function	IDRS Unit Number	Multiple Access	Campus for Manual Refunds
8 - Sacramento	63721	FR and OG	AU, KC, and OG
8 - San Diego	63732	FR and OG	AU, KC, and OG
8 - San Jose	63730	FR and OG	AU, KC, and OG
8 - Seattle	63686, 63687, 63689	FR and OG	AU, KC, and OG
EDCA-ITS, CCI - Managers	63380	Any	N/A
EDCA-ITS, CCI -Covington KY	63376 and 63388	Any	N/A
EDCA-ITS, CCI - Dallas	63384 - 63385, 63402	Any	N/A
EDCA-ITS, CCI - Fresno	63381	Any	N/A
EDCA-ITS, CCI - Memphis	63386-63387, 63345	Any	N/A
EDCA-ITS, CCI - Ogden	63383, 63403	Any	N/A
EDCA-ITS, CCI - Puerto Rico	63382, 63389, 63401	Any	N/A
EDCA-ITS, CCI - St. Louis	63379	Any	N/A
EDCA-ITS, CCI - Seattle	63377 - 63378	Any	N/A
EDSA	63113, 63811, 63813	Any	N/A
ITAP	63120-63129	Any	N/A
LCATS	63393-63397	Any	AU, KC, and OG
Quality Review Program	63710, 63713-63714	Any	N/A
TAG	63102	Any	N/A

Below are the acronyms used in the Multiple Access and Campus for Manual Refunds columns in the table above.

Acronym	Campus
AT	Atlanta
AU	Austin
BR	Brookhaven

Exhibit 13.10.2-9 (Cont. 4) (09-09-2025)
IDRS Multiple Access Approval Table

Acronym	Campus
CI	Cincinnati
FR	Fresno
KC	Kansas City
ME	Memphis
OG	Ogden
PH	Philadelphia

