



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

13.4.2

MARCH 21, 2023

EFFECTIVE DATE

(03-21-2023)

PURPOSE

- (1) This transmits revised IRM 13.4.2, Administration and Security.

MATERIAL CHANGES

- (1) IRM 13.4.2.1.2, added new acronyms and removed those no longer used in this IRM.
- (2) IRM 13.4.2.5.1, updated to clarify completion of TAMIS Employee Screen before submitting a BEARs request.
- (3) IRM 13.4.2.5.5, updated with current password rules based on Password Screen. SERP Feedback #6561.
- (4) IRM 13.4.2.8, clarified example and added (4) and (5) to clarify when a case should not be deleted from the Taxpayer Advocate Management Information System (TAMIS).
- (5) IRM 13.4.2.8.1, clarified only non-bargaining unit employees, specifically the Local Taxpayer Advocate (LTA), acting LTA, Centralized Case Intake (CCI) manager, or acting CCI manager can delete a case from TAMIS and updated the procedures for deleting cases.
- (6) IRM 13.4.2.8.1.1, moved Caution for clarity.
- (7) IRM 13.4.2.8.2, updated to current record retention procedures.
- (8) IRM 13.4.2.8.3(8), moved paragraph to IRM 13.4.2.8.4.
- (9) IRM 13.4.2.8.4, added new section for Case Removal Monitoring by Area Offices and Director CCI.
- (10) IRM 13.4.2.9, added OAR deletion procedures to those currently in use.
- (11) IRM 13.4.2.10, added Reopen Record procedures.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 13.4.2, Administration and Security, dated March 30, 2022. IRM Procedural Update (IPU) 22U0940 (issued 9/9/2022) has been incorporated into this IRM.

AUDIENCE

Taxpayer Advocate Service employees.

Jennifer K. Cones
Acting Executive Director Case Advocacy, Intake and Technical
Support

13.4.2

Administration and Security

Table of Contents

- 13.4.2.1 Program Scope and Objectives
 - 13.4.2.1.1 Responsibilities
 - 13.4.2.1.2 Acronyms
 - 13.4.2.1.3 Related Resources
- 13.4.2.2 TAS Staff Responsibilities
- 13.4.2.3 TAMIS Developers/Database Administrator Responsibilities
 - 13.4.2.3.1 Restricting Access to the TAMIS Database
- 13.4.2.4 Maintaining the Integrity of TAMIS
- 13.4.2.5 TAMIS Access
 - 13.4.2.5.1 Obtaining a Login and Password for TAMIS
 - 13.4.2.5.2 TAMIS Training
 - 13.4.2.5.3 TAMIS Updates
 - 13.4.2.5.4 Security Rules
 - 13.4.2.5.4.1 Idling on TAMIS
 - 13.4.2.5.5 Changing an Existing Password
- 13.4.2.6 Special Situations Requiring Corrections to the TAMIS Employee Screen
 - 13.4.2.6.1 TAS Employees Detailed to Another TAS Office
 - 13.4.2.6.2 New Badge Number or Name Change
 - 13.4.2.6.3 TAS Employee Permanently Reassigned to Another TAS Office
 - 13.4.2.6.4 Permanent Inactive Status
- 13.4.2.7 Permission Levels
- 13.4.2.8 Deleting Cases
 - 13.4.2.8.1 Procedures for Deleting a TAMIS Case
 - 13.4.2.8.1.1 Remove Option
 - 13.4.2.8.2 Case Removal Record Retention
 - 13.4.2.8.3 Case Removal Report Generation, Review and Analysis
 - 13.4.2.8.4 Case Removal Monitoring
- 13.4.2.9 Deleting Operations Assistance Requests
- 13.4.2.10 Deleting a Reopen Record

13.4.2.1
(03-30-2022)
Program Scope and Objectives

- (1) *Purpose:* This section is an overview of the administration and security requirements of the Taxpayer Advocate Management Information System (TAMIS). The section addresses responsibilities of both the Taxpayer Advocate Service (TAS) employees and the Information Technology employees. This section includes procedures for accessing TAMIS, such as obtaining a TAMIS password, access restrictions, basic security rules, and reporting TAMIS problems.
- (2) *Audience:* These procedures apply to all TAMIS users, administrators, and developers.
- (3) *Policy Owner:* The Executive Director Case Advocacy, Intake and Technical Support (EDCA-ITS), who reports to the Deputy National Taxpayer Advocate (DNTA).
- (4) *Program Owner:* DNTA.

13.4.2.1.1
(03-30-2022)
Responsibilities

- (1) The Director of TAS Systems Operations and Support is responsible for the administration and security requirements of TAMIS. See IRM 13.4.2.3, TAMIS Developers/Database Administrator Responsibilities.
- (2) The EDCA-ITS is responsible for establishing policy concerning the use of TAMIS.
- (3) TAS managers are responsible for following the internal control procedures outlined in IRM 13.4.2.2, TAS Staff Responsibilities, IRM 13.4.2.4, Maintaining the Integrity of TAMIS, and IRM 1.4.13.4.9.1, Taxpayer Advocate Management Information System (TAMIS).
- (4) TAS employees are responsible for following IRM 13.4.2.2.

13.4.2.1.2
(03-21-2023)
Acronyms

- (1) The following table contains a list of acronyms used throughout this IRM.

| Acronym | Definition |
|----------|--|
| AMS | Accounts Management System |
| BEARS | Business Entitlement Access Request System |
| CCI | Centralized Case Intake |
| CF | Case File |
| DBA | Database Administrator |
| DEDCA | Deputy Executive Director Case Advocacy |
| DNTA | Deputy National Taxpayer Advocate |
| EDCA-ITS | Executive Director Case Advocacy, Intake and Technical Support |
| ID | Identification Number |

| Acronym | Definition |
|---------|---|
| IDRS | Integrated Data Retrieval System |
| Ind | indicator |
| IRM | Internal Revenue Manual |
| LTA | Local Taxpayer Advocate |
| NBU | non-bargaining unit |
| OAR | Operations Assistance Request |
| Org | Organization |
| OS | Operations Support |
| PID | Personal Identification Number |
| SA | System Administrator |
| TAMIS | Taxpayer Advocate Management Information System |
| TAS | Taxpayer Advocate Service |
| TIN | Taxpayer Identification Number |

13.4.2.1.3
(03-30-2022)

Related Resources

- (1) TAS employees will use the following resources in conjunction with this IRM:
- IRM 1.4.13, TAS Guide for Managers;
 - IRM 13.1, Taxpayer Advocate Case Procedures; and
 - *TAMIS User Guide*.

13.4.2.2
(03-30-2022)

TAS Staff Responsibilities

- (1) TAS managers are responsible for ensuring that all TAS cases are established on the TAMIS database and updated (i.e., closed, transferred etc.) accurately. See IRM 1.4.13.4.9.1, Taxpayer Advocate Management Information System (TAMIS), for more information.
- (2) TAS managers must ensure all personnel designated to access the TAMIS database are properly trained in order to use TAMIS effectively. Refer to IRM 13.4.2.5.2, TAMIS Training, for additional information regarding the training program and the *TAMIS User Guide*.
- (3) The National TAMIS Program Manager serves as the primary liaison between the TAS employees, the host site at the Enterprise Computing Center - Memphis, and the TAMIS developers.

13.4.2.3
(03-30-2022)

TAMIS Developers/Database Administrator Responsibilities

- (1) The TAMIS developers, part of Application Development Internal Management, are responsible for developing the TAMIS application and other application related activities, such as implementing approved program changes, defining the application's workload volume, coordinating the testing, and repairing application problems.
- (2) The Database Administrator (DBA) researches and resolves Oracle and TAMIS database problems. The DBA maintains, monitors and backs up necessary

database files and table space as necessary. If required, the DBA forwards application-based problems and information to the TAMIS developers for resolution.

- (3) Problems submitted to the Operation Support Customer Assistance Line at 866-743-5748 or OS GetServices at <https://selfservice.web.irs.gov/webtier-9.64/ess.do> are forwarded to the DBA .
- (4) TAMIS service hours (TAMIS real-time) are 24 hours per day, seven days a week. The DBA notifies TAS of any scheduled or unscheduled downtime.

13.4.2.3.1 (03-30-2022) **Restricting Access to the TAMIS Database**

- (1) The System Administrator (SA) and DBA are the TAMIS security administrators and are responsible for processing all Business Entitlement Access Request System (BEARS) requests for access to the TAMIS Redesign (DCC Production Platform). They assign initial passwords, and maintain all necessary audit logs.
- (2) The SA and DBA ensure that only authorized personnel are allowed access to the TAMIS database for query, update, and report generation. Field personnel may not alter either the nationally developed programs or the database.
- (3) The SA or the DBA removes a user's access to TAMIS when warranted. For example, employees who no longer require access to TAMIS due to reassignment, separating from TAS, or more than 90 days of inactivity.

13.4.2.4 (03-30-2022) **Maintaining the Integrity of TAMIS**

- (1) TAS managers are responsible for the integrity of the TAMIS database. TAMIS should be monitored to ensure the following:
 - a. All cases are established accurately and timely on the TAMIS database and are properly coded.
 - b. Accurate and timely case coding, including date fields.
 - c. There is no unauthorized removal of cases. If cases are removed, refer to IRM 13.4.2.8, Deleting Cases, for restrictions concerning removal of a case from TAMIS.
 - d. Monitor access to the system. When an employee no longer has a bona fide business need to access TAMIS, submit a BEARS request selecting the option Remove Access to an Entitlement. See IRM 13.4.2.6.4, Permanent Inactive Status.
- (2) The rules and regulations governing unauthorized access apply to all taxpayer systems of records including TAMIS. Individuals may only access TAMIS or individual cases for a bona fide business purpose. Report generation or specialized report writing using Business Objects Enterprise or Tableau should also be conducted on a "need to know" basis.
- (3) Use and sharing of statistics gathered from TAMIS is addressed in IRM 13.5.1, TAS Balanced Performance Measurement System.

13.4.2.5 (05-17-2011) **TAMIS Access**

- (1) This section addresses gaining access to the database and security responsibilities; for example, protecting your password and changing your password, if compromised.

13.4.2.5.1
(03-21-2023)
**Obtaining a Login and
Password for TAMIS**

- (1) To access the TAMIS system, the TAS managers should: .
 - a. Create a TAMIS Employee Screen first. Refer to the *TAMIS User Guide*.
 - b. Then complete a BEARS request.

Note: Completion of the TAMIS Employee Screen first will avoid delays in processing BEARS requests.
 - (2) Within the BEARS system, select 1 TAS Personnel (TAMIS Redesign (DCC Production Platform)) to obtain the appropriate access.
 - (3) Management should review the BEARS request to ensure it is properly completed. In the *Userid* field, enter the employee's TAMIS *Login Name*.
 - (4) Once the BEARS request is approved, you are provided with a temporary password to access TAMIS. You will be prompted to change the temporary password the first time you log in.
- Note:** Temporary passwords are only valid for 24 hours, if you don't create a new password the same day, you may need to submit a BEARS password reset request.
- (5) You are responsible for maintaining the security of your TAMIS password.

13.4.2.5.2
(03-21-2023)
TAMIS Training

- (1) Local Taxpayer Advocates (LTAs) and Centralized Case Intake (CCI) managers must ensure that all TAMIS users are trained in the proper use of the system.
- (2) Operations Support is responsible for TAMIS training coordination.
- (3) Course number 12050, Taxpayer Advocate Management Information System (TAMIS), can be conducted in a variety of methods. Ideally, the training should be taught using computers, allowing for individual hands-on practice. TAMIS can also be taught by combining group discussion with periods of hands-on practice at the student's workstation.
- (4) The TAMIS course is designed to provide the mechanics of using the database. To access the TAMIS Training database, contact your local TAS Training or TAMIS coordinator for login instructions.
- (5) Separate training is available for the TAMIS report-writing software.

13.4.2.5.3
(03-21-2023)
TAMIS Updates

- (1) Director of TAS Systems Operations & Support will coordinate with EDCA-ITS to communicate TAMIS updates to all users when changes are implemented in the TAMIS database. These communications will provide information covering the nature of the TAMIS changes and related user instructions.
- (2) Upon receipts of the communication, managers and employees should read the communication to determine the impact on their case actions. Managers and employees should contact their local TAMIS coordinator if they have questions concerning TAMIS functionality and send questions concerning TAMIS policy to the **TAS TAG Policy and Guidance* mailbox.

13.4.2.5.4
(03-30-2022)
Security Rules

- (1) Protect your TAMIS password and do not reveal it to anyone.
- (2) Never use another person's password.
- (3) Never leave your password in your desk or around your work area.
- (4) Lock the workstation screen, or sign off the system if you leave your workstation for any length of time. Report any suspected compromise or abuse of the system to your local office security representative or management.
- (5) You should always change your password whenever you feel it has been compromised.
- (6) If you have not logged into TAMIS for more than 45 days, you will be "locked out." You must contact the Operation Support Customer Assistance Line at 866-743-5748, or complete a BEARS request selecting "Password Reset". When contacting the help desk or completing the BEARS request, you must provide your TAMIS login.
- (7) If you have not logged into TAMIS within 90 days, your login will be removed from the system; and a new BEARS request must be completed to reinstate your access to TAMIS. See IRM 13.4.2.5.1, Obtaining a Login and Password for TAMIS, for these procedures.
- (8) Your login and password systemically lock after three consecutive unsuccessful attempts at logging in using an incorrect password. To unlock your account, submit an account unlock request via BEARS: select Password Reset and notate in the Special Instructions "account unlock."
- (9) Multiple login processes (i.e., a user being signed on more than once using the same login and password and attempting to conduct two or more TAMIS sessions simultaneously) are not permitted.
- (10) Each user is only allowed one TAMIS user account.

13.4.2.5.4.1
(03-30-2022)
Idling on TAMIS

- (1) "Idling" occurs when a user does not execute a keystroke or when the screen display does not change.
- (2) TAMIS users should sign off TAMIS if there is no need to take any TAMIS actions and/or if there is no need to have continual/uninterrupted access to the database.
- (3) If you are idle for more than 120 minutes (2 hours), you will be signed off. Any unsaved data will be lost.

13.4.2.5.5
(03-21-2023)
Changing an Existing Password

- (1) You may change your password by selecting the *Administration* button from the TAMIS Main Menu, then the *Password* button on the Administration Menu.
- (2) Passwords are case sensitive and must:
 - a. Be between 8 to 16 characters in length.
 - b. Not be the same as the user name.
 - c. Start with an alphabetic character.
 - d. Have at least one lower-case alphabetic character.
 - e. Have at least one upper-case alphabetic character.
 - f. Have one to two numeric characters.
 - g. Have one to two special characters.

h. Differ from the previous password by least three letters.

(3) Valid special characters are as follows:

Special Characters Available for Use in Passwords

| Symbol | Symbol Description |
|--------|-------------------------|
| ! | Exclamation Point |
| - | Hyphen |
| = | Equal Sign |
| . | Period |
| ~ | Tilde |
| _ | Underscore |
| { } | Left and Right Braces |
| [] | Left and Right Brackets |
| : | Colon |

(4) If your password has been compromised, change your password immediately.

13.4.2.6
(03-30-2022)

**Special Situations
Requiring Corrections to
the TAMIS Employee
Screen**

- (1) The Employee Screen is used to record each employee who is authorized to use TAMIS, or has cases assigned to them on the system. Situations occur which require unique modifications to the Employee Screen, such as:
- TAS employee is detailed to another TAS office;,,
 - TAMIS user receives a new badge number or changes his or her name;
 - TAS employee is permanently reassigned to another TAS office; or
 - TAMIS user has to be moved into a permanent inactive status.

13.4.2.6.1
(03-30-2022)

**TAS Employees Detailed
to Another TAS Office**

- (1) If you are detailed to another TAS office, you will need access to TAS cases managed by the detailed-to Organization (Org) code. You must complete a BEARS request, to gain access to the detailed-to Org.

Example: An employee in Org code 28 accepts a detail assignment as an acting group manager in Org code 25. To access the detailed-to office's inventory and assign cases, the acting manager requires login rights to Org code 25.

- (2) *Login names and Employee ID #* cannot be duplicated on another TAMIS Employee Screen.
- (3) Complete a BEARS request to request a new TAMIS login and password for the temporary site. On the BEARS request, Special Instructions field, provide the new TAMIS *Login Name* and advise the system administrator that the existing TAMIS *Login Name* should be disabled (provide the existing *Login Name*).

- (4) Once assigned to the new office, employees will not be able to actively work cases assigned to the losing office Org code. The losing office must reassign all open inventory.
- (5) Update the Employee Screen as follows:
 - a. The Employee Screen at the losing office Org code must be modified. The level 3 or 4 permission user at the losing Org Code must update the Employee Screen, setting the *Inactive Ind* to Inactive.
 - b. A new Employee Screen for the detailed-to Org code must be established. The level 3 or 4 permission user at the detailed-to Org code must add a new Employee Screen using the new temporary employee login with a new *Employee ID #*. The new ID number follows the ID number format DTLxx.

Example: Employee ##-DTLxx is comprised of ## for the Detailed to Org code, DTL to represent the fact the employee is on detail, and xx would be the numbers 00, 01, 02, etc., following a sequence for new detail in employees.

Example: Employee DRHADD28 is on detail to Org Code 29. The employee's *Login Name* on the detailed-to Org Code Employee Screen is DRHADD29, and, if the user is the first detail-in employee, their *Employee ID #* is 29-DTL00.

- (6) The detailed in employee would be given the appropriate permissions, for example, case assignment privileges and the appropriate permission level.
- (7) Once the detail assignment is complete, and the employee returns to their home Org code, their access rights must be reestablished at their home Org code and the temporary detailed-to office must modify the Employee Screen as follows:
 - a. The temporary detailed-to Org code must reassign all open inventory.
 - b. The detailed-to Org code must set the *Inactive Ind* to Inactive.
 - c. The home Org code must update the *Inactive Ind* to Active on the original Employee Screen.
- (8) Upon completion of the temporary assignment, the employee must complete a BEARS request. On the BEARS, Special Instructions field, advise the system administrator to enable the original TAMIS Login Name (and include the login), requesting a new password, and advise that the temporary TAMIS Login Name should be disabled (and include that login). A new temporary password will be provided for the original TAMIS Login Name.

13.4.2.6.2
(03-30-2022)
**New Badge Number or
Name Change**

- (1) If you have been assigned a new badge number (*Employee ID #*), due to a name change, etc., a new Employee Screen must be created.

Note: The only exception to the requirement to create a new Employee Screen when a new badge is issued, is for the initial release of the Smart Card badge. When the Smart Card is issued, enter the Personal Identification Number (PID) in the Employee Screen PID field.

- (2) You cannot modify the *Employee ID #* field. A new Employee Screen must be created, and security modifications input on the old Screen. You do not have to

complete a new BEARS request, to gain access, unless your name has changed as well, which requires access under a new *Login Name*.

- (3) If a new badge was issued **and** there is a new name:
 - a. On the BEARS request, Special Instructions field, provide the new TAMIS *Login Name* and advise the system administrator that the existing TAMIS *Login Name* should be disabled (provide the existing *Login Name*).
 - b. The level 3 or 4 permission user in the Org code must update the Employee Screen of the old/original *Employee ID #* or badge number to permission level 0.
 - c. Do not edit the *Login Name* on the old/original Employee Screen.
 - d. Add a new Employee Screen with the new *Employee ID #* and *Login Name*, including assigning the appropriate permission level.
 - e. Once open inventory is reassigned to the new *Employee ID #*, the *Inactive Ind* on the original Employee Screen must be set to Inactive.
- (4) If there is a new name, but a new badge was not issued:
 - a. On the BEARS request, Special Instructions field, provide the new TAMIS *Login Name* and advise the SA that the existing TAMIS *Login Name* should be disabled (provide the existing *Login Name*).
 - b. The level 3 or 4 permission in the Org code user must update the Employee Screen of the old/original *Login Name* to permission level 0.
 - c. Do not edit the *Login Name* on the old/original Employee Screen.
 - d. Add a new Employee Screen with the new Login name including assigning the appropriate permission level.
 - e. Reassign all open inventories to the new *Employee ID #*. All closed cases will remain on the database under the original *Employee ID #*.
 - f. Due to the requirement for a unique *Employee ID #*, the new Employee Screen displays a modified *Employee ID #*. The first two digits reflect the Org code, followed by a dash, and the remaining 5 characters should be the last 5 digits of the badge number/PID, or if that *Employee ID #* has already been used, on an Employee Screen, follow the same pattern to start the *Employee ID #* with the Org code number then insert add an **N**, for new, followed by the last 4 digits of the badge number or PID, after the Org code.
 - g. Once open inventory is assigned to the new *Employee ID #*, the *Inactive Ind* on the original Employee must be set to Inactive.

Example: Sue L. Maple, badge number 62-45455, of Org code 62 has a name change to Sue L. Apple. She did not receive a new badge. The new *Login Name* is SLAPPL62 and the modified *Employee ID #* is 62-N5455.

13.4.2.6.3
(03-30-2022)
**TAS Employee
Permanently Reassigned
to Another TAS Office**

- (1) If you have been permanently reassigned to another TAS office, you will need a new *Login Name* for the new organization code. Complete a BEARS request to gain access under the new Org code.
- (2) Request a new TAMIS login and password for the new site. On the BEARS request, Special Instructions field, provide the new TAMIS *Login Name* and advise the system administrator that the existing TAMIS *Login Name* should be disabled (provide the existing *Login Name*).
- (3) You may also receive a new badge number, depending on the new location.

- (4) Since you cannot have dual log in accounts or dual *Employee ID #'s* on TAMIS, the following procedures/steps are to be followed by a level 3 or 4 permission user in the losing office:
 - a. The Employee Screen at the losing office Org code must be modified. The level 3 or 4 permission user must update the Employee Screen.
 - b. Reassign open inventory.
 - c. The *Inactive Ind* box must be updated to Inactive.
 - d. The permission level must be changed to 0.
 - e. Insert "employee reassigned" in the street address line.
 - f. Update the local telephone number to the employee's manager's or secretary's telephone number.
 - g. Do not modify the existing login field.
- (5) The gaining office will create a new Employee Screen using the new *Login Name*. Input the new badge number (*Employee ID#*) and IDRS number, if a new badge and IDRS number was issued.
- (6) If the employee is reassigned to a new location and retains the same badge number, the format for the TAMIS *Employee ID #* is *##-Nxxxx*: where *##* equals the Org Code, *N* represents new, and *xxxx* equals the last four digits of the badge number or Smart Card PID.

13.4.2.6.4
(03-30-2022)
**Permanent Inactive
Status**

- (1) If a user does not have a business need to access TAMIS, their Employee Screen must be updated.
- (2) The Employee Screen cannot be removed; instead a level 3 or 4 permission user in the Org code should edit the screen as follows:
 - a. Update the permission level to 0.
 - b. Update the local telephone number to the employee's manager's or secretary's telephone number.
 - c. Update the *Inactive Ind* to Inactive.
 - d. Do not modify the existing *Login Name* field.
- (3) All open inventory must be reassigned.
- (4) The employee or employee's manager must submit a BEARS request to remove the application.

13.4.2.7
(07-28-2020)
Permission Levels

- (1) A permission level is assigned to every employee who is listed on the Employee Screen. See IRM 1.4.13.4.9.1, Taxpayer Advocate Management Information System (TAMIS), for information on assigning TAMIS Permission Levels by position.
- (2) Depending on your permission level, you will be able to view data, add data, or remove data. See IRM 1.4.13.4.9.1.1, Making Deviations from a TAMIS Permission Level, for additional information.
- (3) Level 5 access has been established for four Headquarters employees. The level 5 users can update cases and Employee Screens for any organization code. Generally, the level 5 permission users only assist if the action cannot be input by level 4 users at the affected office.
- (4) Refer to the TAS Permission Levels list on the TAS TAMIS/IRM web page at the following link: *TAMIS Permission Levels*

13.4.2.8
(03-21-2023)
Deleting Cases

- (5) Level 5 permission users have *limited* ability to change codes or the list of values within TAMIS.
- (1) Only Permission Level 4 users within the same TAMIS Org code or a level 5 Super User can delete or remove a case from TAMIS.
 - a. CCI employees retain the Org code on TAMIS of the LTA office in which they are located.
 - b. CCI managers have Permission Level 4 (see IRM 13.4.2.7, TAMIS Permission Levels). Therefore, CCI managers are responsible for reviewing and approving deleted case requests submitted by Intake Advocates reporting to the CCI manager before they delete the case.
- (2) The ability to delete or remove cases is an administrative tool which should be exercised in limited situations. TAMIS case removal should be kept to a minimum. In general, there are only two situations that warrant a case removal:
 - If at the time of case creation, a case was added erroneously to TAMIS.
Example: The taxpayer's problem is already resolved by an Operation's actions, but TAS did not recognize it was resolved.
 - A duplicate case has been added to TAMIS.
Example: The case is identical in the taxpayer's entity to an existing case. If new inquiry has the same entity as the open case and the taxpayer is raising new issue(s) or tax account(s), the new issue(s) or tax account(s) should be added to the existing case.

Reminder: When creating an e-911 on Accounts Management System (AMS) to add a case to TAMIS, dialogue boxes will appear if a case involving the same Taxpayer Identification Number (TIN) is already on TAMIS. A similar dialogue box occurs when loading a case directly to TAMIS. Before continuing with the e-911 or TAMIS records, the employee will review the existing TAMIS case(s) to determine if the issue is a duplicate or possible re-open. See IRM 13.1.16.11, Inquiries on Open and Closed TAMIS Cases.
- (3) TAMIS cases that have specific data imperfections or errors (e.g., incorrect dates, premature closure, erroneous reopen record, or erroneous data in a protected field) should not be removed. Each TAS office should correct these data elements. If errors cannot be corrected by the local office level 4 permission users, elevate the problem to your Area TAMIS Coordinator. If needed, the Area TAMIS Coordinator elevates the problem to Director of TAS Systems Operations & Support by submitting a *Technology Request*.
- (4) TAS employees make a case acceptance determination for AMS referrals from another IRS Operating Division or Function before creating a case on TAMIS. Once a case acceptance determination has been made, TAS will work the case. See IRM 13.1.16.8.5, Referrals from IRS Operating Divisions/Functions. TAS employees will not make another case acceptance determination once the case has been loaded to TAMIS. Remember, the IRS has informed the taxpayer of TAS assistance, and this decision was confirmed by a TAS

employee who worked the AMS referral and accepted the case. **Do not delete cases once they have been established on TAMIS when you disagree with the case acceptance determination.**

- (5) There are times when new information is presented after a case has been loaded to TAMIS, and the taxpayer or representative no longer requires assistance from TAS, or the taxpayer has received relief from the Operating Division or Function. These cases should not be deleted, instead they should be closed as a No Relief Code 54, taxpayer withdraws relief request, or No Relief Code 53, Operating Division or Function already provided relief. See IRM 13.1.21.2.2.26, Withdrawal or Requested Closure of TAS Case, and IRM 13.1.21.2.1.1, Relief Codes.

13.4.2.8.1
(03-21-2023)
**Procedures for Deleting
a TAMIS Case**

- (1) If a TAMIS case warrants removal, the following actions **MUST** be taken prior to removal.
- a. Forward a request for case deletion via secure email to the CCI manager, or LTA. The request should indicate the case file number to be deleted with a detailed reason as to why the case needs to be deleted. Include the duplicate case file number when required.
- Note:** To assist the CCI manager or LTA, consider using the following subject line: Case Deletion Request CF 1234567.
- (2) The LTA, officially designated acting LTA, CCI manager, or officially designated acting CCI manager will determine whether the case should be deleted. When the LTA or CCI manager determines the case will be deleted, they will:
- a. Document TAMIS, copy and paste the email request to delete the case into the TAMIS History to explain the reason for the removal.
 - b. If the case to be removed is a duplicate of a case already on TAMIS, both cases must be documented before the duplicate is removed. Duplicate the History Screen to the original case.

Example: CF# 3603304 is being removed since it is an identical erroneous duplicate of CF #3603302 currently on TAMIS. Add a history CF# 3603304, which is being removed. Create the duplicate history by selecting the Duplicate History button to copy the history to CF# 3603302. An automated history posts that says: "THIS HISTORY WAS DUPLICATED TO CASE 3603302". The case remaining on TAMIS contains the duplicated history referencing the case number that was removed.

- c. Generate and print a hardcopy and electronic copy of Form 911H, for the case to be removed. Print the Form 911H to a .pdf format and name the document with the case number and deletion date, e.g., 1234567-mm-dd-yyyy.pdf. CCI Managers will promptly provide the hardcopy Form 911H to the LTA in the office in which they are located for records retention purposes.
- d. Send the electronic copy of Form 911H via secure email to TAS.TAMIS.Case.Deletions@irs.gov on the same day it is removed from TAMIS. When printing the Form 911H to a .pdf format, name the document with the case number and deletion date, e.g., 1234567-mm-dd-yyyy.pdf. See IRM 13.4.2.8.2, Case Removal Record Retention.

Caution: This direction applies specifically to non-bargaining unit (NBU) employees. The NBU employee **must** be the LTA, officially designated acting LTA, CCI manager, or officially designated acting CCI manager. A bargaining unit employee should not be designated as the person responsible for removing cases from TAMIS.

13.4.2.8.1.1
(03-21-2023)
Remove Option

- (1) Only permission level 4 users, or above can delete/remove a case.

Caution: Once you delete the record, the deletion cannot be reversed.

- (2) Cases are deleted/removed from the Taxpayer Screen.
- (3) To delete the case, query the case in the *Case File #* field.
- (4) Select Record followed by Remove on the menu bar or *Delete Record* from the icon bar.

Note: Reopen cases cannot be removed after the Initial Actions and/or Closing Actions Screens are saved.

- (5) The following confirmation displays:

- *Are you sure you want to delete this case? Select Yes or No.*

13.4.2.8.2
(03-21-2023)
Case Removal Record Retention

- (1) The LTA and CCI manager are the designated NBU officials allowed to remove cases. The LTA and CCI manager should officially designate a back-up NBU employee with TAMIS permission level 4 to this task when absent from the office for more than seven calendar days.
- (2) The LTA retains the hard copy case removal records, including those sent to the LTA from co-located CCI managers. See IRM 13.4.2.8.1, Procedures for Deleting a TAMIS Case.
- (3) Each office should keep a complete hardcopy Form 911H for every case it has removed during the current and prior fiscal years. These records may be requested for validation purposes during an Operational Review. See IRM 1.4.13.9.6.3, Operational Reviews.
- (4) Each office will also send an electronic copy of the Form 911H via secure email to TAS.TAMIS.Case.Deletions@irs.gov.
 - a. Print the Form 911H to a .pdf format and name the document with the case number and deletion date, e.g., 1234567-mm-dd-yyyy.pdf.
- (5) The hardcopy version should be securely stored to prevent any unauthorized browsing or disclosure. Select a secure cabinet location to maintain the printed Forms 911H. Access should be limited to the LTA, NBU secretary, and the employee with TAMIS permission level 4 designated as the responsible person for case deletions and record retention when the LTA is out of the office for more than seven calendar days.
- (6) The retention period for a deleted case record is two years from the end of the fiscal year of case removal. At the end of the retention period these reports should be destroyed. See Document 12990, Records and Information Management Records Control Schedules.

13.4.2.8.3
(03-21-2023)**Case Removal Report
Generation, Review and
Analysis**

- (7) The LTA is required to review the office's case removal report to ensure that a hardcopy Form 911H exists for every listed case removal, to determine the appropriateness of the case removal.
- (1) Reports must be generated and retained to track the removal of cases from the TAMIS database.
- (2) On a semi-monthly basis each office must generate and print a case removal report that lists all cases removed for that time period.
- (3) One report must be run in deletion order to list cases removed from the 1st through the 15th day of the month. The other report must be run to list cases removed from the 16th to the last day of the month.
- (4) The reports should be run within 10 days after the end of the semi-monthly period.
- (5) The report should be associated with the hardcopy Forms 911H for the case listed on the report. These should be retained for the retention period described in IRM 13.4.2.8.2, Case Removal Record Retention.
- (6) Each office must designate an NBU employee (DEDCA, Director, LTA, or designee) to review the office's case removal report to ensure that a hardcopy Form 911H exists for every listed case removal, to determine the appropriateness of the case removal.
- (7) Any knowingly inappropriate or unaccounted for case removal may constitute an unauthorized alteration of taxpayer data.
- (8) Director of TAS Systems Operations & Support generates and retains consolidated national case removal reports.

13.4.2.8.4
(03-21-2023)**Case Removal
Monitoring**

- (1) Area Offices and the Director CCI should generate and retain consolidated case removal reports for all offices within their jurisdiction. It is recommended that case removal review and analysis be part of a local office's operational review. See IRM 1.4.13.9.6.3, Operational Reviews.

Note: The Director CCI (or designee) will have access to the electronic versions of the Form 911-H in order to conduct these reviews.

- (2) Area Offices and the Director CCI will take the following actions each month:
 - a. Extract the deleted case information on the first day of each month for the prior month for each office within the Area and CCI.
 - b. Compare for the electronic version of the Form 911-H with deleted case records on the extraction list to verify the deleted record was preserved as required by IRM 13.4.2.8.1.
 - c. The Area office and Director CCI will review the deleted record(s) by the 15th of each month for the prior month to ensure procedures were followed.
 - d. If procedures were not followed, the Area Office and Director CCI will promptly alert any office to take the required corrective action.

13.4.2.9
(03-21-2023)
**Deleting Operations
Assistance Requests**

- (1) Only Permission Level 4 users within the same TAMIS Org code or a level 5 Super User can delete an Operations Assistance Request (OAR) from TAMIS.
- (2) The ability to delete or remove OARs is an administrative tool which should be exercised in limited situations. TAMIS OAR removal should be kept to a minimum. See IRM 13.1.19, Advocating with Operations Assistance Requests (OARs). In general, OARs should only be removed from TAMIS when the OAR was:
 - a. Created in error or prematurely; and
 - b. Created on TAMIS and never issued.

Caution: Once you delete the OAR, the deletion cannot be reversed.

- (3) The LTA or officially designated acting LTA will determine whether the OAR should be deleted. When the LTA determines the OAR will be deleted, they will document TAMIS explaining the reason for the removal of the OAR. To delete the OAR:
 - a. Select the OAR button and scroll to the OAR to be removed.
 - b. Select Record and Remove from the menu bar or Delete Record from the icon bar.
 - c. The following confirmation displays: *Do you really want to remove this OAR record from the case?* Select Yes or No.

Caution: Do not select the Save Button. If you do, you will generate a new OAR.

13.4.2.10
(03-21-2023)
**Deleting a Reopen
Record**

- (1) Only Permission Level 3 or 4 users within the same TAMIS Org code or a level 5 Super User can delete a Reopen Record from TAMIS.
- (2) The ability to delete or remove a Reopen Record an administrative tool which should be exercised in limited situations. TAMIS Reopen Record removal should be rare. See IRM 13.1.16.11.1, Reopen Procedures. In general, Reopen Records should only be removed from TAMIS when:
 - a. The customer has not provided the previously requested information and the case was reopened prematurely;
 - b. There are no Service errors that warranted the case reopening; or
 - c. The case was reopened in error or was the incorrect case number.

- (3) Reopen Records are removed from the case on the Reopen Screen.

Caution: If you are not on the Reopen Screen, you will delete the Reopen Record **and the original case from TAMIS**. This action cannot be reversed.

- (4) The LTA or officially designated acting LTA will determine whether the Reopen Screen should be deleted. When the LTA determines the Reopen Screen will be deleted, they will document TAMIS explaining the reason for the removal of the Reopen Screen. To delete the Reopen Screen:
 - a. Select the Reopen button.
 - b. Select Record and Remove from the menu bar or Delete Record from the icon bar.

Note: Reopen Records cannot be removed after the Initial Actions and/or Closing Actions Screens have been saved.

- c. The following confirmation displays: *Are you sure you want to delete this record?* Select Yes or No. Once the Reopen Records is removed, the case will default back to closed status.

