MANUAL TRANSMITTAL

2.2.1

Department of the Treasury
Internal Revenue Service

DECEMBER 3, 2019

EFFECTIVE DATE

(01-01-2020)

PURPOSE

(1) This transmits revised IRM 2.2.1, Partnership Control System, Partnership Control System Chapter Overview.

MATERIAL CHANGES

(1) Program Scope and Objectives added.

(2) Terms/Definitions/Acronyms added.

(3) Related Resources added.

(4) Updated 2.2.1.2.4 to remove references to outdated security standards.

EFFECT ON OTHER DOCUMENTS

IRM 2.2.1, dated December 16, 2013, is superseded.

AUDIENCE

This document provides instructions for the general use of the operators accessing the Partnership Control Systems display terminals in the SB/SE, LBI, TE/GE, and Appeals Operation Divisions in the Campuses and Area/Industry Offices.

Nancy Sieger
Acting Chief Information Officer

2.2.1
Partnership Control System Chapter Overview

Table of Contents

2.2.1.1
(01-01-2020)
Program Scope and Objectives

(1) This IRM provides an overview of the Partnership Command Code (PCS) including general IDRS security information.

2.2.1.1.1
(01-01-2020)
Terms/Definitions/ Acronyms

(1) List of terms and definitions used throughout this IRM section

IDRS	Integrated Data Retrieval System
SACS	Security and Communications System
USR	Unit Security Representative
PTI	Production Training Indicator
AIMS	Audit Information Management System
TSID	Terminal Security Identifier

2.2.1.1.2
(01-01-2020)
Related Resources

(1) IRM 2.3.9, *IDRS Terminal Responses, Security Command Codes for IDRS Users*

(2) IRM 10.8.1, *Information Technology (IT) Security, Policy, and Guidance*

(3) IRM 10.8.34, *Information Technology (IT) Security, IDRS Security Controls*

2.2.1.2
(01-01-2011)
Partnership Control System Chapter Overview

(1) This handbook provides instructions for the general use of the operators accessing the Partnership Control System display terminals in the Campuses and Area/Industry Offices.

(2) These instructions provide explicit procedures for entering or extracting data from the Partnership Control System.

(3) The Partnership Control System uses the Integrated Data Retrieval System's (IDRS) Security System. Detailed instructions for the Security System are contained in IRM 2.3.9, IDRS Terminal Responses, Security Command Codes for IDRS Users.

2.2.1.3
(01-01-2011)
IDRS Security System

(1) The Security and Communications System (SACS) provide security and auditing for IDRS.

(2) The IDRS Security System is designed to provide the protection defined in IRM 10.8.1, Information Technology (IT) Security, Policy, and Guidance, and conforms to the various laws and regulations defined in IRM 10.8.34 IDRS Security Handbook, Exhibit 10.8.34-2.

(3) The IDRS Security System provides identification and authorization for every input. • The Employee Security File contains significant data required to recognize each employee authorized to use IDRS. • The Terminal Security File includes terminal identification to recognize each workstation capable of accessing IDRS.

(4) All actions taken on IDRS, both authorized and unauthorized, are recorded in the IDRS audit trail.

(5) The IDRS Security System is designed to provide protection to both the taxpayer and IDRS user.

- The taxpayer must be protected from unauthorized disclosure of information concerning their account as well as unauthorized access, inspection, and changes to it.
- The IDRS user employee must be protected from other personnel using their identification to access or make changes to an account.

2.2.1.3.1
(01-01-2014)
Protection of Taxpayer Accounts

(1) Taxpayers must be protected from:

- Unauthorized disclosures of account information.
- Unauthorized changes of account information.
- Unauthorized accesses (UNAX) to account information.

(2) Employees should exercise special precautions to identify the taxpayer or their authorized representative when answering inquiries about a refund, notice, adjustment or delinquent account.

(3) When responding to telephone inquiries and walk-in taxpayers about a tax account, the employee handling the inquiry should obtain:

a. Taxpayer's name, address.
b. Taxpayer Identification Number (SSN or EIN).
c. Document Locator Number (DLN), date or amount on notice or other document received.
d. Date and/or amount of refund, adjustment, payment or return.
e. Type of notice or other communication received.

(4) If a caller is unable to furnish enough information to establish that he/she actually is the taxpayer, the employee should request that the caller find out the information and call back. If the caller states he/she does not have the information and cannot obtain it, the employee should advise the caller to write to the IRS office that generated the taxpayer correspondence.

(5) Employees shall not provide Taxpayer Identification Numbers over the telephone. Exception: Employees performing duties which require them to provide Taxpayer Identification Numbers over the telephone will follow their functional IRM guidelines (e.g. Employees staffing Toll Free Phone Applications).

(6) Walk-in taxpayers should not be given tax return information until they have properly identified themselves.

(7) Information concerning taxpayers will not be provided to third parties without written authorization from the taxpayer. This is true even when the third party requesting information has possession of a copy of the bill or notice in question.

(8) Written authorization from the taxpayer is not restricted to a power of attorney or to any specific form. The authorization must bear the taxpayer's signature. If there is serious doubt whether the signature on the authorization is the taxpayer's, offer to mail the information to the taxpayer's address of record.

2.2.1.3.2
(01-01-2011)
Protection of the IDRS User

(1) It is equally important that each employee be protected from other personnel using their identification.

a. Users must properly safeguard their password in order to obtain the benefits of the IDRS security system.
b. Users must adhere to established sign-on and sign-off procedure. Proper use of command codes SINON and SINOF will help provide protection to the user.

(2) It is essential that only properly authorized employees have access to IDRS.

a. IDRS access must be requested using the OL5081 application. Requests must be approved by the user's manager and their Unit Security Representative (USR). IDRS user accounts can only be created by a home campus IDRS Security Officer or an IDRS Security User Administrator. For IDRS purposes, the home campus is the location where the user's IDRS account is managed based on the user's business organization.
b. Changes to IDRS user accounts must be input by either the user's Unit Security Representative (USR), their home campus IDRS Security Officer, or an IDRS Security User Administrator. These changes must be approved by the user's manager and their Unit Security Representative (USR). IRM 10.8.34 IDRS Security Handbook defines which changes can be input by a USR and which can only be input by an IDRS Security Officer or IDRS Security User Administrator. IRM 10.8.34 also describes the procedures that must be followed to request changes to user accounts.
c. User profiles should only contain those IDRS command codes necessary to perform their official duties.

2.2.1.3.3
(01-01-2011)
Authorized Access

(1) IDRS users are authorized to access only those accounts required to accomplish their official duties.

(2) IDRS users *must not* access their own or spouse/ex-spouse's account, the account of a friend, relative or any account in which they have a personal financial interest.

(3) IDRS users *must not* access the account of another IRS employee unless it is part of their official duties.

(4) IDRS users *must not* access the account of a celebrity, business, or other prominent individual or entity unless it is part of their official duties.

2.2.1.3.4
(01-01-2020)
Passwords

(1) Each IDRS user will be responsible for creating an IDRS password that is only known by that user, and he/she is responsible for its security.

(2) See IRM 10.8.34.6.1.4 for specific instructions on password management.

2.2.1.3.5
(01-01-2011)
SINON

(1) The command code SINON is used to sign-on to IDRS.

(2) An employee must sign-on to IDRS before accessing or changing any account on IDRS. The employee will accomplish this by inputting Command Code (CC)SINON (See Exhibit 2.2.1-1.) that will verify whether or not the employee is authorized to use IDRS. The sign-on screen contains a brief paragraph explaining the responsibilities and disciplinary actions that may result to all authorized users who misuse the system. A user who signs onto IDRS is ac-

knowledging that they have read and understand the disciplinary statement. After signing on IDRS, users will begin to enter command codes on the IDRS screen.

(3) During sign-in, the user must ensure that the Production Training Indicator (PTI) is set appropriately. PTI's are

- P = for the production mode — no restriction
- T = for the training mode — no restriction
- R = for the research mode — restricted to selected users

A banner across the top of the IDRS Access screen will let the user know if they are signed-on to production, training, or research mode.

(4) The employee's IDRS password is protected from viewing during the sign-on process. This field is not displayed on the screen to help safeguard the password.

(5) If an employee is verified as authorized to access IDRS files, the user will receive access to the "LOGON SUCCESSFUL ..." IDRS screen. This screen provides session information, production type, includes the InfoConnect ID and Terminal Identifier; and provides banner information about unauthorized access to the system and unauthorized access to taxpayer information.

(6) The IDRS Security Officer in the home campus or an IDRS Security User Administrator can adjust the employee's profile for restricted PTI's when the employee needs to obtain access to only one type of account. If no changes are made to the employee's profile, the employee will continue to have access to any type of account. The restricted PTI's are:

- I = restricted access for IMF production accounts only
- B = restricted access for BMF production accounts only
- A = restricted access to IMF research accounts only
- C = restricted access to BMF research accounts only

(7) An employee cannot be signed on to more than one IDRS terminal at a time and cannot be signed on in both the production and training modes at the same time unless the employee is authorized for Dual SINON.

(8) If an employee without Dual SINON is signed onto a terminal and signs on at another IDRS terminal, the employee's IDRS session is automatically closed on the first terminal.

(9) If an employee with Dual SINON signs on a third terminal, the employee's IDRS sessions are closed on the first two terminals and the employee profile is systemically locked.

2.2.1.3.6
(01-01-2011)
Entry Code

(1) As of January 2004:

- IDRS will no longer generate a two-character Entry Code when users sign on IDRS.
- Users will no longer add an Entry Code at the end of each IDRS transaction.

2.2.1.3.7
(01-01-2011)
SINOF

(1) The command code SINOF is used to sign-off IDRS. Proper use of this command code provides protection that the employee's access to IDRS will not be used by others for inappropriate activities and accesses.

(2) Users must use command code SINOF or use the top X in the right corner to sign-off IDRS. Users must sign-off IDRS whenever they are going to be away from their workstation. In situations where users need to be away from their workstation for a brief period of time and it is impractical to sign-off IDRS (ie: they are in the process of inputting an adjustment or generating correspondence using CC LETER), the user should activate their password-protected screen lock to prevent an unauthorized user from accessing their IDRS account.

#

(4) If a user is signed on at one workstation and signs on to another workstation, the user account at the first workstation will be automatically de-activated unless the user has been profiled for Dual Access.

(5) See Exhibit 2.2.1-2 in this IRM for the SINOF input format and input instructions.

2.2.1.3.8
(04-26-2006)
Security Files

(1) The security system provides identification and authorization for every terminal input. The Employee Security File contains significant data required to recognize each employee authorized to use IDRS. The Terminal Security File includes terminal identification to recognize each terminal in the IDRS.

2.2.1.3.9
(01-01-2011)
Training Mode

(1) Training Mode connects employees to an IDRS training system where they can access and modify fake taxpayer accounts.

(2) Employees will be able to update a training account through real-time and then will be able to view the updated effect on the account.

(3) The employee's user profile in Training Mode is different from their employee profile in Production Mode. When signed-on in Training Mode, employees can only use command codes contained in their Training Profile. Employees should contact their manager or USR for instructions on modifying their Training Profile.

(4) All Training Mode actions are recorded in the IDRS audit trail.

(5) All Training Mode security violations will be included in IDRS security reports.

(6) When an IDRS user is signed on in the Training Mode, the terminal will be authorized for the same command codes as the user's Training Profile until he/she signs off.

(7) Training mode accounts may be restored to the original condition by two methods:

a. by terminal input of command code RESTR to restore a specific module, an entire account, or an Audit Information Management System (AIMS) record.
b. by daily (or periodic) restoration of the entire training file.

(8) When operating in the Training Mode on production accounts (research mode), no actual updating of any IDRS data can be made. All command codes, are otherwise used in exactly the same manner as when in the Production Mode.

2.2.1.3.10
(01-01-2011)
Security Violations

2.2.1.3.11
(01-01-2011)
Terminal Security Locks

2.2.1.3.12
(01-01-2011)
General Security Reminders

(1) Users should sign-off IDRS whenever they are going to be away from their workstation.

(2) Users should know their Unit Security Representative (USR), Alternate USRs and Terminal Security Administrators (TSAs) and how to contact them.

(3) Users should know their Terminal Security Identifier (TSID), their Unit Number, and their IDRS Employee Number.

(4) Users should periodically review the IRS Security Rules.

(5) Users should check their user profile regularly for changes.

(6) Users should access only those accounts required to accomplish their official duties.

(7) Users should clear taxpayer account information from their IDRS screen to prevent unauthorized disclosure of taxpayer information.

(8) Users should retrieve all prints immediately from a printer. If someone leaves a print in the printer, it should be removed and shredded or placed into a waste container for disposing of sensitive information if the originator cannot be determined.

2.2.1.3.13
(01-01-2011)
RMODE

(1) Command code RMODE authorizes an employee to use the command codes contained in their Training Profile in a research mode.

(2) The research mode differs from production mode in that production files are accessed but not updated. It differs from training mode in that the training files are not accessed.

(3) The research mode is to be used only by:

a. IDRS User Support staffs for researching production problems that can be resolved only by accessing production data.
b. Application development staffs for addressing issues that can be resolved only by accessing production data. Application development staff use must be in compliance with IRM 10.8.8 Information Technology (IT) Security, Live Data (LD) Protection. Application development staffs must meet all IRM 10.8.8 requirements (including Live Data Request Form approval) before RMODE access will be granted.

(4) In order to use the research capability, a user must have command code RMODE in their Production Profile, and input command code SINON with a Production/Training Indicator of R.

(5) An Audit Trail Record will be produced for all inputs made in the research mode.

This Page Intentionally Left Blank

Exhibit 2.2.1-1 (01-01-2011)
Command Code SINON

SINON Input Screen Format for Original Sign-On

```
    1-9    | 11-19  | 21-29  | 31-39  | 41-49  | 51-59  | 61-69  | 71-80
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
 1 SINON      PTI:  P    SSN OR SEID:                                                                 1
 2 LAST NAME:                                                                                         2
 3 FIRST INITIAL:                                                                                     3
 4 PASSWORD:                PWMGT (SIGNIF. YEAR):                                                     4
 5      TO CHANGE PASSWORD, ENTER ALL REQUIRED FIELDS ABOVE, THEN ENTER NEW                           5
 6      PASSWORD AND CONFIRM NEW PASSWORD BELOW.  PASSWORDS MUST BE 8 TO 12                           6
 7      CHARACTERS.  PASSWORDS MUST HAVE AT LEAST 1 NUMBER AND 1 LETTER.                              7
 8      NO LETTER OR NUMBER MAY BE REPEATED MORE THAN THREE TIMES IN A ROW.                           8
 9      FOR EXAMPLE:   AAA1BBB2   OR   111A222BCD                                                     9
10 NEW PASSWORD:                                                                                     10
11 CONFIRM NEW PASSWORD:                                                                             11
12           *****     INTEGRATED DATA RETRIEVAL SYSTEM     *****                                    12
13                                                                                                   13
14 WILLFUL UNAUTHORIZED ACCESS OR INSPECTION OF ANY TAXPAYER INFORMATION                             14
15 --REFERRED TO AS UNAX--IS EXPRESSLY PROHIBITED.  ACCESS TO THIS SYSTEM IS                         15
16 RESTRICTED TO THOSE EMPLOYEES AND CONTRACTORS WHO HAVE AN AUTHORIZED,                             16
17 WORK-RELATED REASON TO ACCESS AND INSPECT TAXPAYER INFORMATION.  WILLFUL                          17
18 UNAUTHORIZED ACCESS OR INSPECTION OF THE TAXPAYER INFORMATION CONTAINED                           18
19 IN THIS SYSTEM MAY SUBJECT THE OFFENDER TO CRIMINAL PROSECUTION UNDER                             19
20 18 U.S.C. 1030 OR 26 U.S.C. 7213, AND ADMINISTRATIVE ACTION.                                      20
21                                                                                                   21
22           *****     REMEMBER - STOP UNAX IN ITS TRACKS     *****                                 22
23                                                                                                   23
1234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890
    1-9    | 11-19  | 21-29  | 31-39  | 41-49  | 51-59  | 61-69  | 71-80
```


Exhibit 2.2.1-1 (Cont. 1) (01-01-2011)
Command Code SINON

```
    1-9     11-19    21-29    31-39    41-49    51-59    61-69    71-80
12345678901234567890123456789012345678901234567890123456789012345678901234567890
 1 SINON      PTI:  P    SSN OR SEID:  123456789                                  1
 2 LAST NAME:   DOE                                                              2
 3 FIRST INITIAL:   J                                                            3
 4 PASSWORD:  AAA1BBB2      PWMGT (SIGNIF. YEAR):                                4
 5      TO CHANGE PASSWORD, ENTER ALL REQUIRED FIELDS ABOVE, THEN ENTER NEW      5
 6      PASSWORD AND CONFIRM NEW PASSWORD BELOW.  PASSWORDS MUST BE 8 TO 12      6
 7      CHARACTERS.  PASSWORDS MUST HAVE AT LEAST 1 NUMBER AND 1 LETTER.         7
 8      NO LETTER OR NUMBER MAY BE REPEATED MORE THAN THREE TIMES IN A ROW.      8
 9      FOR EXAMPLE:   AAA1BBB2   OR   111A222BCD                                9
10 NEW PASSWORD:                                                                10
11 CONFIRM NEW PASSWORD:                                                        11
12           *****     INTEGRATED DATA RETRIEVAL SYSTEM     *****               12
13                                                                              13
14 WILLFUL UNAUTHORIZED ACCESS OR INSPECTION OF ANY TAXPAYER INFORMATION         14
15 --REFERRED TO AS UNAX--IS EXPRESSLY PROHIBITED.  ACCESS TO THIS SYSTEM IS     15
16 RESTRICTED TO THOSE EMPLOYEES AND CONTRACTORS WHO HAVE AN AUTHORIZED,         16
17 WORK-RELATED REASON TO ACCESS AND INSPECT TAXPAYER INFORMATION.  WILLFUL      17
18 UNAUTHORIZED ACCESS OR INSPECTION OF THE TAXPAYER INFORMATION CONTAINED       18
19 IN THIS SYSTEM MAY SUBJECT THE OFFENDER TO CRIMINAL PROSECUTION UNDER         19
20 18 U.S.C. 1030 OR 26 U.S.C. 7213, AND ADMINISTRATIVE ACTION.                  20
21                                                                              21
22           *****     REMEMBER - STOP UNAX IN ITS TRACKS     *****             22
23                                                                              23
12345678901234567890123456789012345678901234567890123456789012345678901234567890
    1-9     11-19    21-29    31-39    41-49    51-59    61-69    71-80
```


Exhibit 2.2.1-1 (Cont. 2) (01-01-2011)
Command Code SINON

#

#
#
#
#

Exhibit 2.2.1-2 (04-26-2006)
Command Code SINOF

Input Screen Format — use this Command Code to log off.

```
|   |   1-9   |  11-19  |  21-29  |  31-39  |  41-49  |  51-59  |  61-69  |  71-80  |   |
|   |12345678901234567890123456789012345678901234567890123456789012345678901234567890|   |
|---|-----------------------------------------------------------------------------------|---|
| 1 |SINOF                                                                              | 1 |
| 2 |                                                                                   | 2 |
| 3 |                                                                                   | 3 |
| / |                                                                                   | / |
|23 |                                                                                   |23 |
|24 |                                                                                   |24 |
|---|-----------------------------------------------------------------------------------|---|
|   |12345678901234567890123456789012345678901234567890123456789012345678901234567890|   |
|   |   1-9   |  11-19  |  21-29  |  31-39  |  41-49  |  51-59  |  61-69  |  71-80  |   |
```

Record Element Description for Command Code SINOF

Element	Line	Position	Description
1	1	1–5	SINOF