MANUAL TRANSMITTAL

2.8.1

Department of the Treasury
Internal Revenue Service

DECEMBER 15, 2023

EFFECTIVE DATE

(01-01-2024)

PURPOSE

(1) This transmits revised IRM 2.8.1, *Audit Information Management Systems (AIMS), Introduction to AIMS REALTIME Processing*.

MATERIAL CHANGES

(1) IRM 2.8.1 updated to add Acting CIO.

(2) IRM 2.8.1.1 Internal Controls revised to comply with the updated standards.

EFFECT ON OTHER DOCUMENTS

IRM 2.8.1 dated February 22, 2023, is superseded.

AUDIENCE

This IRM is intended for the general use of IDRS system personnel from all four Business Operating Divisions (W&I, SB/SE, LB&I and TE/GE) and Appeals accessing the Audit Information Management System.

Kaschit Pandya
Acting, Chief Information Officer

2.8.1
Introduction to AIMS REALTIME Processing

Table of Contents

2.8.1.1 Program Scope and Objectives
2.8.1.1.1 Background
2.8.1.1.2 Authority
2.8.1.1.3 Responsibility
2.8.1.1.4 Program Management and Review
2.8.1.1.5 Program Controls
2.8.1.1.6 Terms/Definitions/Acronyms
2.8.1.1.7 Related Resources
2.8.1.2 AIMS File Content
2.8.1.3 IDRS Security System
2.8.1.3.1 Protection of Taxpayer Accounts
2.8.1.3.2 Protection of the IDRS User
2.8.1.4 Authorized Access
2.8.1.4.1 Passwords
2.8.1.4.2 SINON
2.8.1.4.3 SINOF
2.8.1.5 EPSF and TPSF
2.8.1.5.1 Training Capabilities
2.8.1.6 Security Violations
2.8.1.6.1 Security Reminders
2.8.1.7 RMODE

Exhibits
2.8.1-1 Command Code SINON
2.8.1-2 Command Code SINOF

2.8.1.1
(12-15-2023)
Program Scope and Objectives

(1) This IRM provides instructions for the use of the Audit Information Management System (AIMS) display terminals in the Campuses or Area Offices. AIMS is using the Integrated Data Retrieval System's (IDRS) Security System. Detailed instructions for administering the IDRS Security System are included in IRM 10.8.34, IDRS Security Controls.

(2) **Purpose** : This transmits revised IRM 2.8.1, Audit Information Management Systems (AIMS), Introduction to AIMS REALTIME Processing.

(3) **Audience**: The audience for this IRM section are users of the Audit Information Management System (AIMS).

(4) **Policy Owner**: Information Technology, Chief Information Officer.

(5) **Program Owner**: Information Technology, Applications Development, Compliance, Business Compliance Management System Branch AIMS Related Section.

(6) **Primary Stakeholders**: IDRS users from Appeals, LB&I, SB/SE, TE/GE and W&I

(7) **Program Goals**: To provide explicit instructions for the use of command codes in entering and extracting data.

2.8.1.1.1
(01-02-2024)
Background

(1) . As a result of a study, it was concluded that Examination had a need for a new information management system. The study group recommended a terminal assisted Audit Information Management System (AIMS). A stand alone direct access terminal system was considered along with the enhancement of IDRS. Enhancement of IDRS was determined to be clearly the best choice for the Service.

(2) This new system satisfied Examination Division's current needs for accurate and timely inventory controls, better control of assessments and up-to-date management reports. The system traces examination results through final determination of tax liability including Appeals and Tax Court.

(3) After the successful implementation of AIMS for the Examination Division, control of returns in Appeals was added to AIMS. As of January 1, 1977 control of Exempt Organization returns was added and on October 1, 1977 control of Employee Plan returns was added.

2.8.1.1.2
(01-02-2024)
Authority

(1) During the summer of 1973, the Deputy Commissioner established a Task Force to identify ADP requirements of Compliance functions, and to make appropriate recommendations to satisfy their needs.

2.8.1.1.3
(02-09-2023)
Responsibility

(1) Headquarters AIMS Related Section is responsible for maintaining procedures related to AIMS programming.

2.8.1.1.4
(01-02-2024)
Program Management and Review

(1) IRS implements access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.

2.8.1.1.5
(01-02-2024)
Program Controls

(1) SACS controls all the IDRS user accesses and permissions.

2.8.1.1.6
(02-09-2023)
Terms/Definitions/ Acronyms

(1) The following table defines acronyms frequently used throughout this IRM section:

Acronyms	Definition
IDRS	Integrated Data Retrieval System
SSN	Social Security Number
EIN	Employer Identification Number
DLN	Document Locator Number
TIN	Taxpayer Identification Number

2.8.1.1.7
(02-09-2023)
Related Resources

(1) EOD, IMF, BMF, EPMF, NMF, RCCMS, RGS

2.8.1.2
(01-01-2000)
AIMS File Content

(1) The AIMS Data Base, Audit Information Management File, contains all the data elements used by the AIMS System.

2.8.1.3
(01-01-2000)
IDRS Security System

(1) The IDRS Security System is designed to provide protection for both the taxpayer and the IDRS user. The taxpayer must be protected from unauthorized disclosure of information concerning his/her account and unauthorized changes to it. The IDRS user must be protected from other personnel using his/her identification to access or make changes to an account.

2.8.1.3.1
(01-01-2000)
Protection of Taxpayer Accounts

(1) The greatest potential for unauthorized disclosure of tax information occurs when IDRS user employees handle telephone inquiries from taxpayers. Employees should exercise special precautions to identify the taxpayer or his/her authorized representative when answering such inquiries. In responding to telephone inquiries, no tax return information may be given out unless it relates to a notice, billing, letter initiated by the IRS, or refund inquiry.

(2) When responding to telephone inquiries about a tax account, the employee handling the inquiry should, at a minimum, obtain the taxpayer's name, address and taxpayer identification number (SSN or EIN). Recipients of calls should continue to ask enough questions to satisfy themselves that they are speaking to the taxpayer. The following are types of information that might be asked the caller:

a. Document Locator Number (DLN), date or amount on notice or other document received.
b. Date and/or amount of refund, adjustment, payment, or return.
c. Type of notice or other communication received.

(3) 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 that a written reply will be mailed to the taxpayer's address of record.

(4) Employees should not provide Taxpayer Identification Numbers over the telephone.

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

(6) Information concerning taxpayers will not be provided to third parties without written authorization from the taxpayer. For example, specific information concerning a client's bill or notice will not be provided to third parties without receipt of written authorization from the taxpayer. This is true even though the third party requesting information has possession of a copy of the bill or notice in question.

(7) 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. Taxpayer Service employees will not request returns from campuses or Federal Records Center solely for verification of 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.

(8) In walk-in contacts, if the third party has possession of a copy of the bill or notice in question, the written authorization should bear the taxpayer's signature and give some indication that the third party is authorized to act for the taxpayer. In the absence of such a written authorization, the third party may only be furnished general information regarding the meaning of the bill or notice. If the third party does not have possession of a bill or notice, the written authorization should bear the taxpayer's name, address and signature and contain information peculiar to the taxpayer of which the third party would not generally be aware. For instance, if the letter or authorization describes a specific refund problem or inquiry with specific facts that only the taxpayer should be aware of, the third party may be given information regarding the refund.

(9) In telephone contacts, Taxpayer Service personnel are restricted to the information they may furnish third parties in the absence of written authorization. Only general information regarding the meaning of a particular notice or letter may be given. Advise the third party to furnish a written authorization in order that information may be provided, or offer to call the taxpayer or mail information to the taxpayer's address of record. Otherwise, no specific information related to the taxpayer or his/her account may be given. No information from IDRS, microfilm, or tax returns may be given to the third party. Naturally, information the third party offers may be accepted. For example, canceled check information may be accepted to initiate a payment tracer on a bill but no information relative to the balance due or nature of the assessment may be given.

(10) When a third party makes a written inquiry, no information may be furnished without written authorization from the taxpayer.

(11) It should be kept in mind that relatives are third parties and the rules outlined in this section apply to them. These rules do not apply to husband and wife

when both sign a joint return. However, when a spouse has been claimed as a dependent on a return (instead of filing jointly) the dependent spouse may not be given information without written authorization from the taxpayer who signed the return.

2.8.1.3.2
(01-01-2005)
Protection of the IDRS User

(1) It is essential that only properly authorized employees have access to command codes since IDRS terminals can be used to change taxpayers' accounts. It is equally important that each employee be protected from other personnel using his/her identification since the only record of the employee making the change will be computer generated from the entry code input by the operator. Proper use of Command Codes SINON and SINOF will provide necessary protection to the employee. However, an employee must properly safeguard his/her password in order to obtain the benefits of the system.

2.8.1.4
(01-01-2000)
Authorized Access

(1) IDRS users are authorized to access only those accounts required to accomplish their official duties. IDRS users must not access their own or spouse's account, the account of a friend, relative or co-workers, or any account in which they have a personal or financial interest.

2.8.1.4.1
(10-23-2006)
Passwords

(1) Each IDRS user will be given a password and he/she is responsible for its security.

(2) Any time a password is compromised, or even if an employee suspects that it has been, he/she will notify the system Security Supervisor to obtain another password. An employee must request a new password if he/she forgets his/her current password.

2.8.1.4.2
(01-01-2005)
SINON

(1) An employee must sign on IDRS before accessing or changing any account on IDRS. The employee will accomplish this by inputting Command Code CC) SINON (see Exhibit 2.8.1–1) that will verify whether or not the employee is authorized to use IDRS.

(2) Immediately prior to signing on, the employee will press any key to determine if the "real-time" system and the terminal are operational. If the real-time happens to go down in the service center before completely inputting CC SINON, the employee should back space through the input. This will clear the sign-on data from the screen. Upon receiving notification that the system is available again, he/she may re-enter CC SINON.

(3) To sign on a terminal the employee will depress (F1). This generates the SINON format with the Production Training Indicator (PTI) which will be P. Next, the Social Security Number (can also use SEID to SINON vs. SSN) and then the name data are input. The password is the last item input before pushing the XMIT key. To protect a password, the employee will tab the cursor to right of the indicator present on the screen.

2.8.1.4.3
(01-01-2005)
SINOF

(1) Employees must use CC SINOF (see Exhibit 2.8.1–2) whenever they are going to be away from the terminal (for example, going to lunch, break, or back to desk). Employees should stay signed on only when they are actively using the terminal or when they can see the terminal and anticipate using it again soon.

(2) Proper use of Command Code SINOF provides employees complete security. If an employee does not SINOF, there is always a danger that someone else will use his/her terminal during his/her absence, and all the actions on the terminal will be recorded as being done by the original employee.

(3) If a user is signed on at a terminal and signs on at another terminal, the original terminal will automatically be deactivated.

2.8.1.5
(01-01-2000)
EPSF and TPSF

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

2.8.1.5.1
(01-01-2000)
Training Capabilities

(1) In the EPSF there will be two profiles recorded, a production profile and a training profile. The production or training indicator in CC SINON determines which profile is used. While operating in the training mode on production accounts, no actual updating of any IDRS data can be made. ALL command codes will be used in exactly the same manner as when in production mode.

(2) Trainees will be able to update a training account through real-time and then be able to recall the account to view the updated affect. Accounts may be restored to the original condition by two methods:

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

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

2.8.1.6
(01-01-2010)
Security Violations

#
#
#
#
#
#
#
#

security lockout, the screen of the affected terminal will display the message "SECURITY LOCK ON THIS TERMINAL" and the terminal keyboard will lock. The operator will immediately notify the IDRS USR (Unit Security Representative) who will initiate action to unlock the terminal.

2.8.1.6.1
(01-01-2000)
Security Reminders

(1) Employees should always clear the screen when the terminal operation is completed.

(2) Employees should be sure to retrieve all prints if the terminal is connected to a printer. If someone leaves a print in the printer, it should be placed in classified waste if the originator cannot be determined.

(3) IDRS terminals are programmed for real-time usage and are systematically deactivated at the end of each work day. Any input at a time not during the authorized time period will be recorded as a security violation.

2.8.1.7
(01-01-2000)
RMODE

(1) Command Code RMODE authorizes an employee to use the command codes contained in his/her Training Profile in a research mode. 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. The research mode is to be used only by the IDRS Control Group and the RPA Staff for researching production problems that can be resolved only by accessing production data. An Audit Trail Record will be produced for all inputs made in the research mode. In order to use the research capability, an employee must have CC RMODE in his/her Training Profile, and input CC SINON with a Production/Training Indicator of R.

Exhibit 2.8.1-1 (01-01-2010)
Command Code SINON

Use this command code to sign on to IDRS. An employee cannot be signed on in both training and production modes at the same time.

#

28249001

```
|   |   1-9    |  11-19   |  21-29   |  31-39   |  41-49   |  51-59   |  61-69   |  71-80   |   |
|   |12345678901234567890123456789012345678901234567890123456789012345678901234567890|   |
|---|-----------------------------------------------------------------------------------------|---|
| 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 |     PASSWORDS CAN NOT CONTAIN SPECIAL CHARACTERS (]@#$%!?)                              |10 |
|11 |NEW PASSWORD:                                                                            |11 |
|12 |CONFIRM NEW PASSWARD:                                                                    |12 |
|13 |          *****     INTEGRATED DATA RETRIEVAL SYSTEM     *****                        |13 |
|14 |                                                                                         |14 |
|15 |WILLFUL UNAUTHORIZED ACCESS OR INSPECTION OF ANY TAXPAYER INFORMATION                    |15 |
|16 |--REFERRED TO AS UNAX—-IS EXPRESSLY PROHIBITED.  ACCESS TO THIS SYSTEM IS                |16 |
|17 |RESTRICTED TO THOSE EMPLOYEES AND CONTRACTORS WHO HAVE AN AUTHORIZED,                    |17 |
|18 |WORK-RELATED REASON TO ACCESS AND INSPECT TAXPAYER INFORMATION.  WILLFUL                 |18 |
|19 |UNAUTHORIZED ACCESS OR INSPECTION OF THE TAXPAYER INFORMATION CONTRAINED                 |19 |
|20 |IN THIS SYSTEM MAY SUBJECT THE OFFENDER TO CRIMINAL PROSECUTION UNDER                    |20 |
|21 |18 U.S.C. 1030 OR 26 U.S.C. 7213, AND ADMINISTRATIVE ACTION.                             |21 |
|22 |                                                                                         |22 |
|23 |          *****     REMEMBER - STOP UNAX IN ITS TRACKS     *****                      |23 |
|---|-----------------------------------------------------------------------------------------|---|
|   |12345678901234567890123456789012345678901234567890123456789012345678901234567890|   |
|   |   1-9    |  11-19   |  21-29   |  31-39   |  41-49   |  51-59   |  61-69   |  71-80   |   |
```

#

Exhibit 2.8.1-1 (Cont. 1) (01-01-2010)
Command Code SINON

#
#
#

Exhibit 2.8.1-2 (01-01-2000)
Command Code SINOF

Use this command code to invalidate assigned entry code.

Input format for Command Code SINOF

	1-10										11-20										21-30										31-40									
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
1	S	I	N	O	F																																			
2																																								
3																																								

Record Element Description for Command Code SINOF

Element	Line	Position	Description and Validity
1	1	1–5	SINOF

Responses:

a. Valid response: REQUEST COMPLETED displayed on line 13.