



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

4.2.9

JULY 6, 2020

## EFFECTIVE DATE

(07-15-2020)

## PURPOSE

- (1) This transmits a new IRM 4.2.9, General Examining Procedures, Integrated Data Retrieval System (IDRS) and Data Security for Examination.

## MATERIAL CHANGES

- (1) This manual provides policies and guidance to Small Business/Self-Employed (SB/SE) Field Examination, Campus Examination, Headquarters Examination, and Examination Specialty Programs, hereby referred to as SB/SE Examination, managers and IDRS Unit Security Representatives to carry out their respective responsibilities regarding security of the Integrated Data Retrieval System (IDRS) and other applications that contain taxpayer data.

## EFFECT ON OTHER DOCUMENTS

none

## AUDIENCE

Small Business/Self-Employed, Campus Examination, Field Examination, Headquarters Examination, and Examination Specialty Programs, Managers and IDRS Unit Security Representatives.

Carol L. Madison  
Director  
Small Business/Self Employed Examination Case Selection



4.2.9  
IDRS and Data Security for Examination

**Table of Contents**

- 4.2.9.1 Program Scope and Objectives
  - 4.2.9.1.1 Background
  - 4.2.9.1.2 Authority
  - 4.2.9.1.3 Roles and Responsibilities
  - 4.2.9.1.4 Program Management and Review
  - 4.2.9.1.5 Program Controls
  - 4.2.9.1.6 Terms/Definitions
  - 4.2.9.1.7 Acronyms
  - 4.2.9.1.8 Related Resources
- 4.2.9.2 IDRS Security Role Designations and Responsibilities
  - 4.2.9.2.1 IDRS Unit Security Representative (USR)
  - 4.2.9.2.2 IORS Report Reviewer
  - 4.2.9.2.3 Alternative Unit Security Representative (USR)
  - 4.2.9.2.4 Terminal Security Administrator (TSA)
  - 4.2.9.2.5 Front Line Manager of IDRS Users
- 4.2.9.3 IDRS User Support
- 4.2.9.4 Establishing IDRS Units
  - 4.2.9.4.1 Maximum Profile Authorization File (MPAF)
  - 4.2.9.4.2 Modify IDRS Units
  - 4.2.9.4.3 Delete IDRS Units
- 4.2.9.5 Transferring Employees Between IDRS Units
- 4.2.9.6 Transferring Employees Within Same Business Organization (Different Campus)
- 4.2.9.7 Transferring Employee Within Same Business Organization (Same Campus, Different OI)
- 4.2.9.8 Transferring Employees to Another Business Organization (Same Campus)
- 4.2.9.9 Transferring Employee to Another Business Organization (Different Campus)
- 4.2.9.10 Technical Services
- 4.2.9.11 IDRS Command Codes and Usage
  - 4.2.9.11.4 Sensitive Command Code Combinations
- 4.2.9.13 Automated Command Code Access Control / Restrictions
- 4.2.9.14 IDRS Online Reports Services (IORS)
- 4.2.9.15 Types of IORS Reports

#  
#  
#  
#

- 4.2.9.15.1 Weekly Security Reports (No Certification Required)
- 4.2.9.15.2 Monthly Security Reports (No Certification Required)
- 4.2.9.15.3 Weekly Security Reports (Certification Required)
- 4.2.9.15.4 Monthly Security Report (Certification Required)
- 4.2.9.16 Report Level Certification
- 4.2.9.17 IDRS Unit and USR Database (IUUD)
- 4.2.9.18 Form 13230, IDRS Security Personnel Designation
- 4.2.9.19 Security Audit and Analysis System (SAAS)
- 4.2.9.20 Form 11377/11377-E Taxpayer Data Access
- 4.2.9.21 Online 5081 (OL5081)
- 4.2.9.22 Password Management (PWMGT)
- 4.2.9.23 IDRS Multiple Accesses Capability (CMODE)
- 4.2.9.24 Security Command Codes - Table and Definitions
- 4.2.9.25 RSTRKA Report
- 4.2.9.26 Unauthorized Access (UNAX)
- 4.2.9.27 Control-D Web
- 4.2.9.28 Integrated Automation Technologies (IAT)
- 4.2.9.29 Account Management Services (AMS)
- 4.2.9.30 New User Orientation Package

Exhibits

- 4.2.9-1 Security Violations Report
- 4.2.9-2 Sensitive Access (Other/Spouse) Report
- 4.2.9-3 Monthly IDRS Security Profile Report
- 4.2.9-4 Report Level Actions
- 4.2.9-5 User Support Issues

4.2.9.1  
(07-06-2020)  
**Program Scope and Objectives**

- (1) Purpose: This IRM section provides policies and guidance to carry out respective responsibilities regarding security of the Integrated Data Retrieval System (IDRS) and other applications, which contain taxpayer return and return information.
- (2) Audience: This IRM is directed toward Small Business/Self Employed (SB/SE), Campus Examination, Field Examination, Headquarters Examination and Examination Specialty Programs, Managers and IDRS Unit Security Representatives. The audience includes the following operations:
  - Campus Examination
  - Field Examination
  - Headquarters Examination
  - Examination Specialty Programs
  - Planning and Special Programs (PSP)
  - Technical Services (East, West, Mid-States, Legacy)
- (3) Policy Owner: The Director, SB/SE Examination is responsible for issuing policy.
- (4) Program Owner: The program owner is Examination Case Selection.
- (5) Primary Stakeholders: Area-wide SB/SE Examination IDRS Security Representatives in North Atlantic, Central, South Atlantic, Midwest, Gulf States, Western, Southwest, Specialty and Campus Examination/Automated Underreporter Program (AUR).
- (6) Program Goals: The primary goal of this IRM is to provide procedural guidance, which will ensure consistency across the organization. This includes the timely review and certification of security reports, addressing user support inquiries not detailed in another IRM.
- (7) Contact Information: To recommend changes or make any other suggestions related to this IRM section, see IRM 1.11.6.6, Providing Feedback About an IRM Section - Outside of Clearance.

4.2.9.1.1  
(07-06-2020)  
**Background**

- (1) IRM 4.2.9, IDRS and Data Security for Examination, further defines requirements found in IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance, and IRM 10.8.34, Information Technology (IT) Security, IDRS Security Controls. In the event of a discrepancy, information in IRM Part 10 takes precedence.
- (2) The IRM 10.8.34.3.1.3, Information Technology (IT) Security IDRS Security Controls, Roles and Responsibilities, Manager, states the managers of IDRS users are responsible for day-to-day implementation and administration of IDRS security in their group. However, to relieve administrative burden on front line managers, SB/SE Examination established dedicated Unit Security Representatives (USRs).
- (3) USRs are responsible for ensuring all aspects of data security are followed and coordinating with the unit manager where issues may arise.

4.2.9.1.2  
(07-06-2020)  
**Authority**

- (1) The following three IRMs define overall IDRS security requirements.
  - a. IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance.

- b. IRM 10.8.2, Information Technology (IT) Security, IT Security Roles, and Responsibilities.
- c. IRM 10.8.34, Information Technology (IT) Security, IDRS Security Controls.

(2) In the event of a discrepancy, information in IRM Part 10 takes precedence over this IRM unless requirements within this IRM are more comprehensive.

4.2.9.1.3  
(07-06-2020)  
**Roles and Responsibilities**

- (1) The USR is responsible for providing IDRS security support and carrying out security duties within their designated Examination Area. Managers of employees who have access to IDRS are responsible for all activities performed on IDRS are within an employee's required tax administration duties.
- (2) IRM 10.8.34.3, Roles and Responsibility, further defines the roles of the Unit Security Representative (USR), Alternative USR, Terminal Security Administrator (TSA), and group manager.

4.2.9.1.4  
(07-06-2020)  
**Program Management and Review**

- (1) SB/SE Examination IDRS Unit Security Representatives, and managers of employees who have access to IDRS and other systems with taxpayer and employee information are required to implement security policies and procedures to help ensure protection of taxpayer data.
- (2) USRs and unit managers shall:
  - a. Monitor and review IDRS Online Reports Services (IORS) reports and Security Audit and Analysis System (SAAS) work products to ensure security reports are thoroughly reviewed and timely certified.
  - b. Collaborate with IT Cybersecurity personnel to address emerging issues.
  - c. Utilizes resources to analyze trends of potential threats, misuse or unauthorized access to taxpayer data.
  - d. Conduct annual operational reviews and develop an annual action plan for the Area USR.

4.2.9.1.5  
(07-06-2020)  
**Program Controls**

- (1) The IORS application will maintain a record of all certifications by the Primary Report Reviewer for each report requiring certification and for each IDRS unit under the Primary Report Reviewer's responsibility.
- (2) Business organizations shall achieve at least a 90% certification rate for their security reports. As outlined in IRM 10.8.34.6.3.1.2, Review and Certification of Security Reports in IORS.
- (3) Cybersecurity IDRS Security Analysts shall:
  - a. Review IORS utility reports to determine whether IORS Primary Report Reviewers in their campus domain(s) are reviewing IDRS Security reports in a timely manner, certifying the reports, and taking the appropriate action, as needed.
  - b. At least weekly provide business organizations in their campus domain(s) with a report listing uncertified reports.
  - c. Work with business organizations in their campus domain(s) to address IDRS security report certification related issues.
  - d. Advise business organizations within their campus domain(s) of any units where a Primary Report Reviewer has not been designated.

- (4) IDRS Security Program Management Office shall perform a compliance review of IDRS security report certifications at least once every six months to determine the certification rate and timely certification rate of business organizations.

4.2.9.1.6  
(07-06-2020)  
**Terms/Definitions**

- (1) The following are terms used in this IRM.

<b>Term</b>	<b>Definition</b>
Audit Trail	A chronological record of transactions entered on IDRS or related applications.
Automated Command Code Access Control	A feature designed to prevent IDRS users with certain roles from having specified command codes in their profiles. i.e., use command codes RSTRK or BYPAS.
Campus domain	A controlled area of IDRS campuses and their servers.
Certification	Refers to the process by which security reports have been analyzed, reviewed, documented and verified as appropriate.
Command Code	A five-character terminal input on IDRS to extract a specific set of data or used to input an action.
Definer	The sixth character of a command code used to extract specific data.
Head of Office Designee	Designated personnel who oversees Form 11377, Taxpayer Data Access.
Security Event	An event that could potentially be an unauthorized attempt to the security of IRS systems or data.
Unit Manager	Supervisor or Acting Supervisor of IDRS Users

4.2.9.1.7  
(07-06-2020)

(1) The following are acronyms used in this IRM.

**Acronyms**

<b>ACRONYM</b>	<b>DEFINITION</b>
AMS	Accounts Management Services
AUR	Automated Underreporter
BOD	Business Operating Division
BU	Bargaining Unit
CC	Command Code
CFOL	Corporate Files On-Line
DD	Discovery Directory
DUL	Designated User List
ECC-MEM	Enterprise Computing Center - Memphis
ECC-MTB	Enterprise Computing Center - Martinsburg
EOPs	Enterprise Operations
ERCS	Examination Returns Control System
FAS	Functional Automation Support
HOD	Head of Office Designee
IAT	Integrated Automation Technologies
IDRS	Integrated Data Retrieval System
IORS	IDRS Online Reports Services
IT	Information Technology
IUUD	IDRS Unit and USR Database
LB&I	Large Business and International
MeF-RRD	Modernized e-File Return Request and Display
MPAF	Maximum Profile Authorization File
NBU	Non-Bargaining Unit
OI	Office Identifier
OL5081	Online 5081
PWACT	Password Activation
PWMGT	Password Management
SAAS	Security Audit and Analysis System
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TDS	Transcript Delivery System

ACRONYM	DEFINITION
TE/GE	Tax Exempt Government Entities
TIN	Taxpayer Identification Number
TSA	Terminal Security Administrator
TSID	Terminal Security Identification
UCCP	Unit Command Code Profile
UNAX	Unauthorized Access
USR	Unit Security Representative

4.2.9.1.8  
(07-06-2020)  
**Related Resources**

- (1) IRM References:
  - IRM 2.3, IDRS Terminal Responses.
  - IRM 2.4, IDRS Terminal Input.
- (2) Website References:
  - CFOL Express at: <http://serp.enterprise.irs.gov/databases/job-aids/misc/cfol-express.pdf>
  - Exam USR SharePoint site at: [https://organization.ds.irsnet.gov/sites/SB/SEfeEPD/ERS/USR/\\_layouts/15/start.aspx#/SitePages/Home.aspx](https://organization.ds.irsnet.gov/sites/SB/SEfeEPD/ERS/USR/_layouts/15/start.aspx#/SitePages/Home.aspx)
  - Document 6209, IRS Processing Codes and Information at: <http://serp.enterprise.irs.gov/databases/irm.dr/current/6209/6209.html>
  - IDRS Command Code Job Aid at: <http://serp.enterprise.irs.gov/job-aids/command-code/command-code.html>.
  - IDRS Online Report Services (IORS) at: <https://iors.web.irs.gov>.
  - IDRS Unit and USR Database (IUUD) at: <https://iors.web.irs.gov/HomeIUUD.aspx>.
  - Taxpayer Data Access Library at: <https://portal.ds.irsnet.gov/sites/PGLD11377/Assets/home.aspx>.
  - IDRS Data Security - Exam Contact List at: <http://serp.enterprise.irs.gov/databases/who-where.dr/idrs-data-security-exam.html>

4.2.9.2  
(07-06-2020)  
**IDRS Security Role Designations and Responsibilities**

- (1) IDRS Security Role Designations and Responsibilities are delegated to individuals responsible for overseeing IDRS Security.
- (2) This IRM section focuses on four security role designations and responsibilities pertinent to IDRS security. They are:
  - Unit Security Representative (USR)
  - IORS Primary Report Reviewer
  - Alternate USR
  - Terminal Security Administrator (TSA)
- (3) For more information on security roles and responsibilities for specific security personnel, operations and functions, see IRM 10.8.34.3, Roles and Responsibilities.

4.2.9.2.1  
(07-06-2020)  
**IDRS Unit Security Representative (USR)**

- (1) The IDRS Unit Security Representative (USR), is an individual assigned by their Business Operating Division (BOD) to implement and administer IDRS security at the IDRS unit level. The USR is sometimes referred to as the "Primary USR," when there are designated Alternate USRs.
- (2) To meet the criteria of a USR, the individual must:
  - Be a Non-Bargaining unit (NBU) employee.
  - Have a completed Background Investigation (BI).
  - Prior to performing USR duties, complete initial training course number 29776, IDRS Unit Security Representatives (USRs).
  - Annually, complete training course number 29862, IDRS Unit Security Representative (USR) Refresher.
  - Be designated by management via Form 13230, IDRS Security Personnel Designation.
  - Certify to Enterprise Operations (EOPS) IDRS Security Accounts Administrator that they have completed the required initial and/or annual refresher training.
  - Be in an IDRS unit where they do not have permissions on IORS to review or certify their own transaction(s) on IDRS.
  - Be a member of a designated IDRS unit that contains all security command codes needed to perform their duties.
  - Submit the Online (OL5081) to have security command codes added to their profile and to have their IDRS account profiled with permissions to support users on all SB/SE home campuses for both the Enterprise Computing Center at Martinsburg (ECC-MTB), and Enterprise Computing Center at Memphis (ECC-MEM).
- (3) The USR must be able to:

Perform:	Such as:
<p><b>Administrative Tasks</b></p>	<ul style="list-style-type: none"> <li>• Explain all IDRS security procedures and instructions prior to adding new users on IDRS.</li> <li>• Perform security awareness training when requested by group/unit manager.</li> <li>• Support the program goals of IT Cybersecurity by providing assistance, analysis and recommendations for action to SB/SE Examination.</li> <li>• Coordinate with management and USRs from all Areas to support reorganizations through the SB/SE Request for Organizational Change process.</li> <li>• Supervise a range of IDRS unit numbers aligned with SB/SE Examination, as outlined in IRM Exhibit 10.8.34-13, IDRS Organization Codes - SB/SE Area.</li> <li>• Conduct regular communication with IDRS users, and unit managers to keeps them abreast of IDRS updates, best practices, new implementations, etc.</li> </ul>

Perform:	Such as:
<p><b>Routine Tasks</b></p>	<ul style="list-style-type: none"> <li>• Add/delete command codes to/from employee profiles with management approval, except for security command codes.</li> <li>• Monitor users' command code usage/non-usage and take action to remove unneeded command codes.</li> <li>• Unlock IDRS workstations and notify the manager of any questionable activity to cause the workstation to be locked.</li> <li>• Process OL5081 requests to add/delete or modify employee IDRS accounts.</li> <li>• Prepare and submit Form 9937, IDRS Unit Request, on IDRS Online Reports Services (IORS) to establish/delete IDRS units, and to modify unit profiles.</li> <li>• Initiate audit trails, via Form 9936, Request for Audit Trail Extract, and ensure employees are aware of audit trails.</li> <li>• Oversee the processing of Form 13230, IDRS Security Personnel Designation.</li> <li>• Transfer employees between IDRS units within their designated Area, and when requested by the unit manager.</li> <li>• Grant IDRS users access to other IRS campuses' databases, i.e. (Multiple Accesses Capability- CMODE).</li> <li>• Add/delete the restriction role on Revenue Agents (GS-512), Tax Compliance Officers (GS-526), Estate Tax Attorneys (GS-905) and HQ Analysts.</li> <li>• Maintain a tracking system of active IDRS users, IDRS unit numbers, Users' Terminal Security Identifications (TSID), and managers and acting managers.</li> <li>• Maintain a centralized storage of Form 11377 and Form 11377-E, Taxpayer Data Access, as the Head of Office Designee (HOD).</li> <li>• Delete users promptly when access to IDRS is not needed.</li> <li>• Lock user's profile immediately if user is on leave for more than 15 days and the user has not implemented the user self-lock feature (LOKME).</li> <li>• Unlock user's profile as requested by the user or manager.</li> <li>• Encourage IDRS users to use the IDRS LOKME feature, which enable users to be pro-active in managing their access to IDRS.</li> <li>• Review IDRS security reports and take appropriate action.</li> <li>• Monitor sensitive command code usage.</li> <li>• Maintain security reports, manuals and handbooks in a locked cabinet when not in use.</li> <li>• Encourage the activation and use of IDRS Password Management in lieu of submitting an OL5081 Password Reset request.</li> <li>• Modify the terminal on/off time to coincide with management approval.</li> </ul>

Perform:	Such as:
<b>Monthly Tasks</b>	<ul style="list-style-type: none"> <li>Review the Automated IDRS Sign-offs Report, Monthly IDRS Security Profile Report, and Password Management Report and take necessary action.</li> </ul>
<b>Quarterly Tasks</b>	<ul style="list-style-type: none"> <li>The review of the Quarterly RSTRK A Report by Office Identifier (OI) and unit range on IDRS.</li> <li>The review of the IORS Quarterly reports for informational use and for planning and analysis purposes.</li> <li>The review of information on the <i>IDRS Unit and USR Database (IUUD)</i> and submit corrections/updates via e-mail to EOPs Security Accounts Administrators to reflect current information. If a manager is on an acting assignment for less than 60 days, the IUUD does not need to be updated.</li> </ul>

4.2.9.2.2  
(07-06-2020)

**IORS Report Reviewer**

- (1) The IORS Report Reviewer is an individual assigned by their business organization to review IDRS security reports in IORS.
- (2) There are two IORS Report Reviewer roles:
  - IORS Primary Report Reviewer
  - IORS Secondary Report Reviewer
- (3) The Primary Report Reviewer
  - Designation is made on Form 13230, IDRS Security Personnel Designation.
  - Is a non-bargaining unit employee.
  - Is either the unit manager or the USR.
  - Is responsible for certifying IORS reports.
  - May grant secondary permissions to authorized personnel.
  - May grant a proxy to authorized personnel.
- (4) The Secondary Report Reviewer:
  - Receives permissions from a Primary Report Reviewer to view one or more security reports for a unit or units.
  - Is a non-bargaining unit employee.
  - Can be a bargaining unit employee if approved by management and authorized by EOPs Security Account Administrators. See IRM 10.8.34.3.2.11.2, IORS Secondary Report Reviewer, for more detailed information.
  - Is usually the manager of an IDRS unit.
  - Cannot certify security reports.
  - Cannot grant permissions to other IORS users to view security reports.

4.2.9.2.3  
(07-06-2020)

**Alternative Unit Security Representative (USR)**

- (1) Alternate USRs assist and/or perform the duties of the Primary USR as a collateral duty assignment.

- (2) Alternate USRs must be approved by a second level manager within the direct chain of command of the IDRS users.
- (3) Alternate USRs can be a bargaining unit or non-bargaining unit employee.

<b>Bargaining unit Alternate USR</b>
Cannot act as Primary USR and cannot perform the full duties of a USR; they support the USR by performing some non-managerial duties.
Cannot review another IDRS user’s actions on IORS, but may have access to IORS reports that do not show employee’s actions on IDRS, such as: Weekly Reports - Employee Count, Master Register (Active) and Monthly Reports - Automated IDRS Sign Off and Password Management Activations
Cannot certify IORS reports.
Is authorized to have all security command codes.

<b>Non-bargaining unit Alternate USR</b>
Is authorized to act as the Primary USR and can review and certify IORS report
May perform all related security duties when officially acting as the Primary USR
Is authorized to have all security command codes

4.2.9.2.4  
(07-06-2020)  
**Terminal Security Administrator (TSA)**

- (1) A Terminal Security Administrator (TSA) is assigned by their business organization to provide additional IDRS user support in unlocking IDRS users’ profiles and terminals only.
- (2) A TSA may be a bargaining unit or non-bargaining unit employee.
- (3) A TSA must receive security training from a current USR.
- (4) A TSA designation is made on Form 13230, IDRS Security Personnel Designation.

#  
#  
#

4.2.9.2.5  
(07-06-2020)  
**Front Line Manager of IDRS Users**

- (1) The Front-Line Manager of IDRS Users:
  - a. Has overall responsibility for IDRS security within their unit to help ensure all activities performed on IDRS by their employees are business related.
  - b. Approves OL5081s for employees in their unit.
  - c. Works in conjunction with the USR regarding the Weekly and Monthly IORS reviews and certifications.
  - d. Coordinates with the USR to establish new IDRS units that falls under their jurisdictions.
  - e. Notifies USR immediately when users within their unit no longer need IDRS access.
  - f. Notifies USR when an employee transfers in or out of the unit.
  - g. Reinforces compliance with security awareness guidelines.

- h. Ensures all employees annually recertify the security rules via OL5081.
- i. Reviews the appropriate use of the command codes in the Maximum Profile Authorization File (MPAF), and employee profiles at least monthly.
- j. Ensures that all requirements associated with a disciplinary action have been met prior to reinstating an IDRS user.
- k. Ensures questionable activity or potential UNAX violations are timely reported to Treasury Inspector General for Tax Administration (TIGTA).

(2) Front line Managers of IDRS users may also:

- a. Request secondary permissions on IORS to view and document security reports for their employees.
- b. Be designated as an Alternate USR or TSA, if officially authorized by an approved Form 13230, IDRS Security Personnel Designation.

4.2.9.3  
(07-06-2020)  
**IDRS User Support**

(1) The USR is the first point of contact for IDRS users at the unit level and must:

- a. Establish a means of communicating with users via e-mail, Skype, centralized mailbox, or a combination of communication sources.
- b. Assist users in a timely manner.
- c. Be able to effectively troubleshoot users' issues by utilizing tools and resources available, such as the IRM 10.8.34, IDRS USR Reference Guide, priority alerts, IDRS Security Program website, IDRS Message Board, etc.
- d. Be able to apply analytic skills to resolve issues.
- e. Be able to translate instructions in written form and to interpret procedures and guidelines to effectively communicate to end users.
- f. Be proficient in USR duties and responsibilities.

(2) Exhibit 4.2.9-5 identifies common types of user support issues. For a list of IDRS security frequently asked questions and answers, refer to the IDRS Security Program link: <http://idssecurity.web.irs.gov/IDRS/IDRSSecurityFAQ.asp>

4.2.9.4  
(07-06-2020)  
**Establishing IDRS Units**

(1) IDRS units are established based on the Internal Revenue Service (IRS) business organization structure. Each business organization i.e., Small Business/Self-Employed, Wage and Investment, Large Business and International, and Tax-Exempt and Government Entities, has an assigned Organization Code Range. For SB/SE Examination, the Organization Code Range, Organization, Function and Unit Number Range are shown in IRM Exhibit 10.8.34-13: IDRS Organization Codes Overview - SB/SE Headquarters & Area Offices.

(2) To establish an IDRS unit, the USR must make sure that the unit number is consistent with the function area as defined in the Treasury Integrated Management (TIMIS) and within the IDRS unit range and organization code as defined by IRM 10.8.34, IDRS Security Controls.

(3) An IDRS Unit Number is a five-digit number that is categorized as follows:

- First and second digits is the Office Identifier( OI) and represent the IRS campus, business organization or Area Office
- Third, fourth, and fifth digits represent the organization code assigned to the campus, business organization or Area Office

- (4) The chart below list SB/SE Field Examination campuses and Area Offices.

OI	CAMPUS	SB/SE AREA	AREA NAME
21	Brookhaven	Area 201	North Atlantic
22	Cincinnati	Area 202	Central
23	Philadelphia	Area 203	South Atlantic & Headquarters
24	Cincinnati	Area 204	Midwest
25	Memphis	Area 205	Gulf States
26	Ogden	Area 206	Western
27	Ogden	Area 207	Southwest
35	na	na	International

- (5) In SB/SE Examination, all units in the same territory should be kept within the same block of numbers and to the extent possible, should be sequenced by group, i.e., the fifth digit of the unit number should be the same as the group number as shown in the organization code structure.
- (6) IDRS units must not contain employees from different business organizations or Area Offices.
- (7) An IDRS unit may consist of one or more IDRS users who are in the same territory, group, or section. Example: When an employee group only has a few IDRS users, users from the same territories may be included in the same IDRS unit. This is known as a “mixed” IDRS unit (employees report to different managers but are in the same territory.) A mixed IDRS unit is established to control single users in one IDRS unit.
- (8) No unit shall have a manager or USR in the same IDRS unit as the employees they oversee.
- (9) The USR must coordinate with the manager to create or assign an IDRS unit that falls under the managers’ jurisdictions.
- (10) Request to establish an IDRS unit is made on Form 9937, IDRS Unit Request, via IORS.

4.2.9.4.1  
 (07-06-2020)  
**Maximum Profile  
 Authorization File  
 (MPAF)**

#  
 #  
 #  
 #



- 4.2.9.6  
(07-06-2020)  
**Transferring Employees Within Same Business Organization (Different Campus)**
- (1) When an employee transfers within the same business organization to a different campus, an OL5081 is required to delete the employee from their current campus. If the employee still needs access to IDRS in their new campus, the employee should contact their assigned USR for further instructions.
  - (2) The gaining USR shall assist the manager and employee with the transfer.
  - (3) The user will also need to request to have their terminal pointed to the new campus.
- 4.2.9.7  
(07-06-2020)  
**Transferring Employee Within Same Business Organization (Same Campus, Different OI)**
- (1) When an employee transfers within the same business organization, on the same campus with a different Office Identifier (OI), an OL5081 is not required.
  - (2) The gaining USR is responsible for transferring the employee's IDRS account to the new unit.
- 4.2.9.8  
(07-06-2020)  
**Transferring Employees to Another Business Organization (Same Campus)**
- (1) When an employee transfers to another business organization within the same campus with a different Office Identifier, an OL5081 is not required.
  - (2) The gaining and losing USR must coordinate to transfer the employee's account to the appropriate IDRS unit.
- 4.2.9.9  
(07-06-2020)  
**Transferring Employee to Another Business Organization (Different Campus)**
- (1) When an employee transfers to another business organization on a different campus, an OL5081 is required to delete the employee from their current campus. If the employee still need access to IDRS in their new BOD, the employee should contact their assigned USR for further instructions.
  - (2) The gaining USR may assist the employee with the transfer.
- 4.2.9.10  
(07-06-2020)  
**Technical Services**
- (1) Technical Services provide technical and procedural support to Field Examination.
  - (2) Technical Services was realigned under four Examination Field Areas:
    - Central- East
    - South Atlantic- Legacy
    - Midwest- Mid-States
    - Western- West
  - (3) The USR for the aforementioned areas shall provide full IDRS security support to Technical Services employees and managers.
  - (4) IDRS units established for Technical Service employees shall fall within the Organization unit range of 680 – 699. See IRM Exhibit 10.8.34-13, IDRS Organization Codes Overview - SB/SE Headquarters & Area Offices

#  
#  
#


#  
#  
#  
#  
#  
#

4.2.9.11  
(07-06-2020)  
**IDRS Command Codes  
and Usage**

- (1) The USR must coordinate with the unit manager to delete command codes from employees' profiles that are unauthorized and/or not being used or needed for their work assignment or position title.
- (2) The USR must query their units to identify units that contain security command codes to ensure security command codes are only in units approved by management to function as USRs, Alternate USRs or TSAs.
- (3) The USR must review the status of Alternate USRs and TSAs on a yearly basis to determine if they are still performing back-up USR support. If no longer providing support, ensure the security command codes are removed from the user's profile.
- (4) The USR must review the MPAF to determine if the command codes in the UCCP and Limited Profile are appropriate for the work performed by the users in the unit.

4.2.9.11.1  
(07-06-2020)

#  
#  
#  
#  
#  
#  
#  
#

4.2.9.11.2  
(07-06-2020)

#  
#  
#  
#  
#  
#  
#  
#  
#  
#  
#









- (5) The Primary Report Reviewer shall not be the reviewer of their own transactions and shall not appear as the IORS Primary Reviewer on the IUUD for the unit that they are in.
- (6) Managers of IDRS users may be designated as Secondary Report Reviewers and can view, add comments, and print IORS reports for their assigned unit.
- (7) To review IORS reports, command code REPTS is required in the report reviewer's IDRS profile.
- (8) Managers who only need IDRS to review IORS reports are put in IORS specific units, i.e. XX900- XX910.

4.2.9.15  
(07-06-2020)  
**Types of IORS Reports**

- (1) There are four weekly security reports available to authorized report reviewers. They are:
  - Employee Count
  - Master Register of Active IDRS Users
  - Security Violations
  - Sensitive Access (Other/Spouse)
- (2) There are three monthly reports available to authorized report reviewers. They are:
  - Automated IDRS Sign-offs
  - Monthly IDRS Security Profile Report
  - Password Management Activations

4.2.9.15.1  
(07-06-2020)  
**Weekly Security Reports  
(No Certification  
Required)**

- (1) **Employee Count:** This report lists the number of active users in each unit. The USR must review this report and take necessary action, such as deleting units that do not have active users and are no longer required.

**Note:** A unit should not be deleted until the Monthly Report has been certified and the subsequent Monthly Report shows no employees assigned to unit.

- (2) **Master Register (Active):** This report identifies all active IDRS users by name, IDRS employee number, Social Security Number (SSN), along with information of user's time on IDRS, time in their currently assigned unit and the status of the user's background investigation date. This report also includes IDRS users' Standard Employee Identifier (SEID) and telephone contact number which is helpful to identify case owners on IDRS. The USR shall take the following actions to rectify this report:
  - a. Validate each unit in the Master Register to identify discrepancies.
  - b. Take corrective actions necessary, such as, moving users between units, updating phone number in IDRS, and confirming approved pseudonym names.

4.2.9.15.2  
(07-06-2020)  
**Monthly Security  
Reports (No Certification  
Required)**

- (1) **Automated IDRS Sign-Offs Report:** This report lists those users whose IDRS sessions terminated after 120 minutes of inactivity. The USR shall take the following actions:
  - a. a. Identify IDRS users with more than 15 automatic sign-offs in a month.
  - b. b. Advise those users to sign-off IDRS when not in use to prevent an unauthorized access.

- c. Instruct user how to periodically refresh their IDRS session by using command code RFRSH, if IDRS is not required on a continuous basis.

- (2) **Password Management Activations Report (PWMGT):** This report lists the number of users in each unit who have activated this capability. Where a unit fails to reflect a 100% activation rate, the USR must research IDRS to identify users who have not activated Password Management and take the following actions:
  - a. Send an e-mail to the user with instruction on how to activate the Password Management Capability.
  - b. Follow-up to ensure that the activation was successful.

See IRM 4.2.9.22, Password Management, for more information on this IDRS feature.

4.2.9.15.3  
(07-06-2020)  
**Weekly Security Reports  
(Certification Required)**

- (1) **Security Violations Report:** This report must be certified within 14 calendar days after the report date for the certification to be considered timely. This report shows accesses made by users on IDRS that generated a security violation. In most cases, security violations occur because of employee error. However, repeated errors for specific violations should be discussed and corrective measures taken to help reduce the number of errors. See Exhibit 4.2.9-1.

- (2) **Sensitive Access (Other/Spouse) Report:** This report must be certified within 14 calendar days after the report date for the certification to be considered timely. This report identifies users who have attempted to or who have accessed other employees' or the spouses/ex-spouse of other employees' accounts. Before this report can be certified, each Social Security Number (SSN) on this report must be researched to determine if the access to other IRS employees' accounts and/or their spouses' accounts, was business related. See Exhibit 4.2.9-2.

4.2.9.15.4  
(07-06-2020)  
**Monthly Security Report  
(Certification Required)**

- (1) **Monthly IDRS Security Profile Report:** The Monthly Security Profile Report provides a summary of all transactions performed on IDRS by end users. This report must be certified within 28 calendar days after the report date for the certification to be considered timely. See Exhibit 4.2.9-3.

4.2.9.16  
(07-06-2020)  
**Report Level  
Certification**

- (1) Certification of security reports is mandatory. After the review and documentation of reports, the USR must complete the Report Level Items as shown in Exhibit 4.2.9-4.
- (2) Level action, comments and certification will apply to all units.

4.2.9.17  
(07-06-2020)  
**IDRS Unit and USR  
Database (IUUD)**

- (1) The IUUD Database is a resource where employees can obtain current information about IDRS units and IDRS security personnel.
- (2) The IUUD is designed to assist employees, managers and security personnel to locate IDRS users and their managers associated with their five-digit IDRS unit number.
- (3) The IUUD also identifies the Primary USRs, Alternate USRs, Primary IORS Report Reviewers, TSAs, and managers for all IDRS units within a business organization.

- (4) The USR is responsible for ensuring the accuracy of the information on the IUUD. To accomplish this, the USR shall:
  - a. Review their assigned units at least once a month and submit updates and corrections to EOPs Security Account Administrators
  - b. Utilize the Employee Count Report on IORS to determine units where there are no employees and submit Form 9937 to mark units as deleted or inactive on the IUUD.

**Note:** A unit should not be deleted until the Monthly Report has been certified and the subsequent Monthly Report shows no employees assigned to unit.

- c. Timely submit Form 13230, IDRS Security Personnel Designation, to update USR, Alternate USR, IORS Primary Report Reviewer, or TSA when their role designation change.

4.2.9.18  
(07-06-2020)  
**Form 13230, IDRS  
Security Personnel  
Designation**

- (1) Form 13230 was developed for IRS Managers to designate individuals within their business organization, the ability to perform IDRS security related activities.
- (2) All individuals requesting the security role designation of Unit Security Representative, IORS Primary Report Reviewer, Alternate Unit Security representative, and Terminal Security Administrator, must submit Form 13230 to EOPs Security Account Administrators for approval.
- (3) Form 13230 must be approved by second-level management or higher.
- (4) A current initial USR Training Certificate or USR Refresher Training Certificate must accompany this form. A certificate is considered current if training was taken within six months from the date Form 13230 was last submitted for approval.
- (5) When the security personnel will provide USR security coverage to more than one IDRS Campus, a separate Form 13230 is required for unit coverage for that campus.
- (6) The order in which to provide IDRS security coverage for a unit or units are as follows:
  - The unit(s) must be established. See IRM 4.2.9.4, Establishing IDRS Units, for more information on establishing a new unit.
  - Form 13230 is submitted to designate USR, Alternate USR, TSA, and IORS Primary Report Reviewer coverage for the unit(s).
  - An OL5081 must be submitted to request security command codes for new security personnel.

4.2.9.19  
(07-06-2020)  
**Security Audit and  
Analysis System (SAAS)**

- (1) All audit trail records, as well as IDRS audit logs, are available for review and analysis in the SAAS Data warehouse by authorized users. Security reviews in SAAS may be expanded at any time to include additional applications.
- (2) SAAS provides on-line analytical processing access to audit trail data to detect security violations.
- (3) Business units are responsible for reviewing SAAS audit trails and certifying accesses to taxpayer data.

## 4.2 General Examining Procedures

- (4) The SB/SE Examination Operations USRs are responsible for the review and certification of security events that appear on the Transcript Delivery System (TDS) and the Modernized e-File (MeF)-RRD reports.
  - (5) A security event is not classified as a security violation or an incident but could potentially be an unauthorized attempt to the security of IRS systems or data.
  - (6) The Cybersecurity staff will e-mail the USR an Open Access report, weekly, and an Access to Employee report for MeF and TDS when available.
  - (7) The Open Access report is subject to a sample review and certification. The business organization determines the sample percentage, which is subject to change.
  - (8) The Access to Employee report is subject to 100% review and certification by the USR.
  - (9) The USR must generally certify sample reports within 14 calendar days of receipt. Management may approve longer certification dates, as appropriate.
  - (10) Certification procedures are the same for both the SAAS reports and the IORS reports. The USR is required to research each Taxpayer Identification Number (TIN) to determine if the access is business-related AND validate that the access is supported by one of the following:
    - Direct case assignment.
    - Related case assignment.
    - Evidence of cross compliance checks.
    - Department of Justice or other official requests.
    - Confirmed input error supported by the identification of another assigned case with similar Taxpayer Identification Number (TIN), such as a transposition or formatting error.
    - A detailed justification statement from the manager when the group or certain employees work assignments will generate reoccurring accesses on this report.
  - (11) When there is no direct case assignment, but the case is controlled on ERCS, the USR shall validate the access.
  - (12) If the USR is unable to certify an access through independent research or managerial response, the USR must submit a referral to TIGTA for follow-up in accordance with IRM 10.8.34.6.3.1.2.3, Security Reports Requiring Certification by a Primary Report Reviewer.
  - (13) Unlike IORS, SAAS does not have the capability to capture review comments. Therefore, the USR shall maintain their completed report, with comments, in a saved file for a length of time as prescribed by your business organization. Certification results are submitted to IT Cybersecurity as directed.
- 
- (1) Employees may use this form to document accesses to taxpayer information when not supported by direct case assignments.
  - (2) This form can also be used when accesses are performed in error or may raise a suspicion of an unauthorized access. False statements may lead to additional inquiries or charges.

4.2.9.20  
(07-06-2020)  
**Form 11377/11377-E**  
**Taxpayer Data Access**

- (3) Employees are authorized to access taxpayer information to perform their official tax related duties and assignments.
  - (4) Employees are not authorized, under any circumstances, to initiate an access to their own tax information or that of other individuals or businesses when they have a personal or outside business relationship where the access could cause or create the appearance of a possible conflict of interest.
  - (5) Employees are required to review the Privacy Act Notification on Form 11377.
  - (6) Use of Form 11377 or Form 11377-E is voluntary.
  - (7) The manager must forward the completed Form 11377/11377-E, to the Head of Office Designee (HOD), by close of business or as soon as possible.
  - (8) In SB/SE Examination Operations, the HOD is the Area Office's assigned USR. To locate the Area's Office HOD, please refer to the UNAX Website: <https://portal.ds.irsnet.gov/sites/vl003/RelatedResources/BU-Head-of-Office-Designees-Form-11377-11377E.pdf>
  - (9) Form 11377-E shall be sent to the HOD via secure e-mail.
  - (10) Copies of Form 11377 or Form 11377-E containing taxpayer data, may not be retained by the employee or the employee's manager.
  - (11) The USR shall review all Forms 11377/11377-E to ensure proper completion and shall upload Forms to the Taxpayer Data Access Library's SharePoint Site including any attachments.
  - (12) Form 11377/11377-E must be uploaded on SharePoint within five business days of receipt and are retained for six years from the upload date.
  - (13) All Forms 11377 received by United States mail, shall be scanned by the USR. If the USR does not have the ability to scan Form 11377, then the USR shall file these forms in a secure location with a retention period of six (6) years from the upload date as required in Document 12990, IRS Records Control Schedules (RCS) 29, Item 270 to ensure the National Archives and Records Administration (NARA) approved records disposition prevents unauthorized/unlawful destruction of records.
  - (14) The naming convention of Form 11377/11377-E is: SEID-MMDDYYYY-##.
    - SEID of the accessing employee.
    - MMDDYYYY is the date of the access, even if the form is completed after the access. Example: January 1, 2020 will be 01012020.
    - ## is the number of forms submitted in sequence on the same day for the same accessing employee. For example, 01 represents the first submission, 02 represents the second submission, etc., for the same accessing employee on the same day.
  - (15) The USR must respond promptly to requests from Labor Relations or TIGTA and provide copies of any Form 11377/11377-E requested for an ongoing investigation.
- 4.2.9.21  
(07-06-2020)  
**Online 5081 (OL5081)**
- (1) The OL5081 Application streamlines the request process for adding, deleting, modifying and password resets for authorized IRS employees to get access to IRS systems.

- (2) Employees access the OL5081 application on the IRS Intranet website *https://ol5081.enterprise.irs.gov*.
- (3) (3) The following is SB/SE Field Examination IDRS Applications by Campus:
  - Area 201 – North Atlantic - **IDRS-BIRSC (IDRS)**
  - Area 202 – Central - **IDRS-CIRSC (IDRS)**
  - Area 203 – South Atlantic - **IDRS-PIRSC (IDRS)**
  - Area 204 – Midwest - **IDRS-CIRSC (IDRS)**
  - Area 205 – Gulf States - **IDRS-MIRSC (IDRS)**
  - Area 206 – Western - **IDRS-OIRSC (IDRS)**
  - Area 207 – Southwest - **IDRS-OIRSC (IDRS)**
- (4) The following is Specialty Program IDRS Applications by Campus:
  - Area 212 – Employment – **IDRS-BIRSC (IDRS), IDRS-CIRSC (IDRS), IDRS-MIRSC (IDRS), IDRS-OIRSC (IDRS)**
  - Area 213 – Estate & Gifts — **IDRS-BIRSC (IDRS), IDRS-CIRSC (IDRS), IDRS-OIRSC (IDRS), IDRS-PIRSC (IDRS)**
  - Area 214 – Excise – **IDRS-BIRSC (IDRS), IDRS-CIRSC (IDRS), IDRS-MIRSC (IDRS), IDRS-OIRSC (IDRS), IDRS-PIRSC (IDRS)**
  - Area 217 – BSA - **IDRS-BIRSC (IDRS), IDRS-CIRSC (IDRS), IDRS-MIRSC (IDRS), IDRS-OIRSC (IDRS)**
- (5) The OL5081 shall not contain Sensitive PII Data such as the employee's social security number.
- (6) The USR and manager have permissions to approve, deny or return a request.
- (7) The manager approving the OL5081 must:
  - Determine whether the employee or the manager will initiate the OL5081 request to be added to an IDRS Campuses' application.
  - Enter the five digits unit number in the "User IDRS Number" field. This field populates a list of USRs or Alternate USRs authorized to process the request. It is important that the unit number is entered correctly so that the request is routed to the correct approval group. The IDRS unit number is the first five digits of the employee's IDRS ten-digit Employee Number and is the unit number assigned by the USR to the manager for their employees.
  - Provide the Enter on Duty (EOD) date in the "Additional Special Instructions" field for new IDRS users.
- (8) The USR approving the OL5081 must:
  - Verify that the correct IDRS campus was selected.
  - Verify that the employee does not have an active IDRS account on another campus.
  - Verify that the correct unit number is shown in the "User IDRS Number" field and make corrections deemed appropriate.
  - Enter the Background Investigation Date in the "Additional Special Instructions" field for returning IDRS users and verify that the manager provided the EOD date in this field for new IDRS users.
  - Ensure the employee's OL5081 completes processing and place any role restriction on the employee's IDRS profile account as applicable.

4.2.9.22  
(07-06-2020)  
**Password Management (PWMGT)**

- (1) Password Management is a feature on IDRS that enables users who have forgotten their IDRS password to get a new temporary IDRS password without having to submit an Online 5081 request.
- (2) PWMGT greatly reduces the number of temporary passwords issued by EOPS Security Account Administrators and saves users wait time of having a temporary password issued.
- (3) USRs shall strongly encourage all users to activate IDRS Password Management.
- (4) USRs shall review the monthly Password Management Activations report on IORS to identify IDRS users who have not activated this feature.
- (5) Command Code PWACT (Password Activation), allow users to activate Password Management.
- (6) Command Code PWMGT (Password Management), allows users who have forgotten their user-generated password to generate a new temporary password.
- (7) Once signed on IDRS with the temporary password, the user will be prompted to change the temporary password to a user-generated password.

4.2.9.23  
(07-06-2020)  
**IDRS Multiple Accesses Capability (CMODE)**

- (1) CMODE is a non-profiled command code and does not have to be put in an IDRS user's profile.
- (2) Command code CMODE enables IDRS users to access other campuses' database without having to sign off IDRS.
- (3) If the IDRS user has not been authorized access to another campuses' database, the attempted use of the command code will not result in a security violation for the user.
- (4) CMODE requires that the IDRS user keep their same user profile and command codes from their home campus when accessing other campuses' databases.
- (5) IDRS users shall be authorized by their managers and approved by their USRs to have CMODE privileges.
- (6) The USR shall grant users permission to access other campuses with command code UPEMP and Definer "S." The permissions will appear as "Authorized Foreign Accesses" on IDRS.
- (7) Users may transfer their profile from one database to another, by entering command code CMODE along with the approved location acronym or Office Identifier. The campus and the field Exam Location Codes and Office Identifiers are:

Campus	Alpha Location Code	Campus Exam Office Identifier	Field Exam Office Identifier
Andover	AN	08	n/a

Campus	Alpha Location Code	Campus Exam Office Identifier	Field Exam Office Identifier
Austin	AU	06	n/a
Brookhaven	BR	01	21
Ogden	OG	04	26 / 27
Philadelphia	PH	05	23
Atlanta	AT	07	n/a
Cincinnati	CI	02	22 / 24
Fresno	FR	10	n/a
Kansas City	KA	09	n/a
Memphis	ME	03	25

- (8) When the IDRS user completes the work on a campus database, the user may enter CMODE and the location acronym or office identifier to go to another approved campus' database, or to return to their home campus database location. IDRS users may also sign off IDRS while their profiles are pointed to another campus' database.

4.2.9.24  
 (07-06-2020)  
**Security Command Codes - Table and Definitions**

#  
#  
#  
#  
#  
#  
#  
#


#  
#  
#  
#  
#  
#  
#  
#  
#  
#





4.2.9.26  
(07-06-2020)  
**Unauthorized Access  
(UNAX)**

- (1) Unauthorized Access (UNAX) is the willful unauthorized access or inspection of taxpayer information, both electronic and paper, and is a crime, punishable upon conviction, by fines, prison terms and termination of employment.
- (2) IRS policy only allows employees to access tax returns and return information when the information is needed to carry out their tax administration duty.
- (3) USRs will perform reviews of security reports to help detect unauthorized (UNAX) activities on IDRS and other systems that employees use to access taxpayer information.
- (4) USRs are responsible for IDRS security. Any IDRS user found not to be following security rules, shall be advised and counseled by management and appropriate action must be taken immediately.
- (5) If an IDRS Security personnel, USR, manager, or other report reviewer encounters any indication of illegal or improper activity, he/she shall refer the case and findings to the proper management and/or TIGTA officials. For the telephone number of your local TIGTA office, view the *map* on their website.
- (6) IRS employees are never authorized to access their own records or records of:
  - their spouse and ex-spouses;
  - their children;
  - their parents;
  - anyone living in their household;
  - their other close relatives;
  - friends or neighbors with whom they have close relationships;
  - celebrities, when the information is not needed to carry out tax related duties;
  - an individual or organization for which they or their spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee, or member;
  - any other individual or organization with which they may have a personal or outside business relationship that could raise questions about their impartiality in handling the tax matter. When employees are working authorized assigned cases or making personal or telephonic contacts, they can access other IRS employees' tax records. However, when the employee working the authorized case knows the other IRS employee, the case must be referred to management for reassignment.

4.2.9.27  
(07-06-2020)  
**Control-D Web**

- (1) Control-D Web (sometimes referred to as Web Access) is a web-based software that allows viewing of reports electronically.
- (2) Control-D Web reduced the requests for prints at campuses and it allows faster access and greater report management for IDRS users.
- (3) IDRS Campus sites no longer print command code TRPRT requests. IDRS users who need a TRPRT print will need to get prints using Control-D Web.

- (4) Control-D Web access server guarantees a secured environment for accessing and viewing reports, and it verifies users and passwords before allowing report access.
- (5) Inactivity during an active session causes a time-out and terminates the session. This prohibits unauthorized viewers when users neglect to log out or lock their workstation.
- (6) All employees and managers will gain access to Control-D Web via the Online 5081 process.
- (7) For additional information on Control -D Web, refer to: *<http://mits.web.irs.gov/idse/>*.

## 4.2.9.28

(07-06-2020)

**Integrated Automation Technologies (IAT)**

- (1) IAT is an application that interacts with IDRS to streamline the IDRS research and input processes.
- (2) IAT requires less manual input making research and case actions more efficient and accurate.
- (3) IAT uses IDRS to gather and submit data. If IDRS is down, or a command code is down, IAT will not function, or may function improperly.
- (4) IDRS users may use IAT to retrieve and research account information. Most tools will not be available if the user is not signed on IDRS.
- (5) USRs may use the Managerial Tool feature in IAT to perform more than one update at a time to employees' profiles in a unit, such as:
  - a. Adding or removing IDRS command codes.
  - b. Locking or unlocking employees' profiles.
- (6) Individual updates to an employee's profile can also be performed using this tool, such as:
  - a. Moving an employee from one unit to another.
  - b. Updating employee telephone number.
- (7) To get IAT, employees may install through the Symantec Software Portal, or submit a ticket through OS GetServices and request the Integrated Automation Technologies (IAT) software.
- (8) For additional information on IAT, refer to the application's website *<https://organization.ds.irsnet.gov/sites/WiMttlai/home/default.aspx>*.

## 4.2.9.29

(07-06-2020)

**Account Management Services (AMS)**

- (1) AMS is a web-based application that emphasizes the sharing of business data and provides a consolidated and synchronized view of taxpayer data and contact information from various IRS systems.
- (2) Many IDRS users request access to AMS. USRs should know the following:
  - a. To access the AMS System, an Online 5081 and registration to the Employee User Portal (EUP) is needed. The requester should contact their manager to determine which application to request.
  - b. AMS users must have command codes TXMOD, ENMOD, INOLE and SUMRY in their individual profiles to use the application.

- (3) USRs may identify users who use AMS by querying command codes AISDL, DMSDL in IORS.
- (4) When a TIN is entered into AMS, the AISDL command is issued, and a LINDX command is issued. The AISDL is audited to the user, the LINDX is not. On successful AISDL, if the user is profiled for Disclosure, a DMSDL command code will be issued and audited to the user.
- (5) The IDRS Automated Command Code Access Control prevents IDRS users with certain roles from having specified command codes in their profiles. If a user is not profiled for an adjustment command code in IDRS they will be restricted from performing adjustment actions in AMS.
- (6) An employee must sign on IDRS before they open the AMS program. When they are finished with AMS, they can just close the AMS window. However, the AMS program does not automatically sign the employee off IDRS. The user is responsible for signing off IDRS outside of AMS.
- (7) For additional information on AMS, refer to the application's website <http://ams.web.irs.gov/index.asp>.

4.2.9.30  
(07-06-2020)  
**New User Orientation  
Package**

- (1) The USR shall e-mail first-time IDRS users an "Orientation Package" that includes but not limited to the following information:
  - a. The user's IDRS unit number.
  - b. The USR's contact information.
  - c. Instructions on how to obtain a Terminal ID (TSID), if applicable.
  - d. Instructions on how to process Form 11377 or Form 11377-E, Taxpayer Data Access.
  - e. Instructions on how to Activate and use the Password Management feature on IDRS.
  - f. IDRS Security Rules and Guidance.
  - g. IDRS Command Code Job Aid website link on SERP.

**This Page Intentionally Left Blank**

**Exhibit 4.2.9-1 (07-06-2020)**  
**Security Violations Report**

Where the report shows four or more of the same violation types made by a user, the USR is required to take appropriate actions as follows:

If four or more of the same violation types...	Then...
<ul style="list-style-type: none"> <li>• PASSWORD MISMATCH</li> <li>• NAME MISMATCH</li> <li>• (PVMGT) SINON ERROR</li> <li>• (PVMGT) RESPONSE ERROR</li> </ul>	<p>Research to determine if the issue has been resolved. If the issue is still outstanding, send an e-mail to the user and/or user's manager to confirm the following:</p> <ul style="list-style-type: none"> <li>• The user committed these errors.</li> <li>• The violations were not the result of an unauthorized attempt to access IDRS.</li> <li>• The user was able to successfully sign on IDRS.</li> </ul> <p><b>Note:</b> The user does not agree they committed the violations, or the USR research identify possible illegal or improper activity, the USR shall refer their findings to the Treasury Inspector General for Tax Administration (TIGTA) officials. For the telephone number of your local TIGTA office, view the map on their website, <a href="https://irssource.web.irs.gov/Linked%20Documents%20Library/TIGTA_complete.pdf#search=tigta%20map">https://irssource.web.irs.gov/Linked%20Documents%20Library/TIGTA_complete.pdf#search=tigta%20map</a>.</p>

**Exhibit 4.2.9-1 (Cont. 1) (07-06-2020)**  
**Security Violations Report**

If four or more of the same violation types...	Then...
CC NOT IN PROFILE	<ol style="list-style-type: none"> <li>1. Research the user's profile to determine if the Command Code (CC) was added since the run date of the report. If added, no further action required.</li> <li>2. Determine if the CC is in the unit's Maximum Profile Authorization File (MPAF).</li> <li>3. If CC is in the MPAF, e-mail the user's manager advising of the security violation made by their employee and to determine if the CC should be added to the user's profile.</li> <li>4. If the CC is not in the MPAF, determine if the CC is authorized for SB/SE Examination Operations' use.</li> <li>5. If authorized, e-mail the user's manager advising of the security violation made by their employee and to determine if the CC should be added to the unit's MPAF.</li> <li>6. If manager approves to have the CC added to the unit's MPAF, submit Form 9937 via IORS. Also, ensure that the manager advises their employees to perform an SFDISP on IDRS to determine what CCs are in their profile and available for use.</li> <li>7. If not authorized, email the user's manager advising of their employee's attempt to use a command code that is not authorized for their position. Include in the e-mail supporting documentation to support your findings.</li> <li>8. Ask the manager to determine why the employee attempted to use the command code and to determine if the violation is non-critical or if further investigation is warranted.</li> </ol>

**Exhibit 4.2.9-1 (Cont. 2) (07-06-2020)**  
**Security Violations Report**

If four or more of the same violation types...	Then...
PROFILE LOCKED	<ol style="list-style-type: none"> <li>1. Research the employee's profile to determine the current status.</li> <li>2. If the employee's profile is unlocked since the run date of the report, no further action required</li> <li>3. If the research shows: <ol style="list-style-type: none"> <li>a. <b>SYS_LOCK</b>: Determine the lock date. The <b>USR</b> shall delete the employee's profile if it is locked for more than twenty-eight (28) consecutive calendar days, unless the manager has knowledge that the employee will have a definite need to access <b>IDRS</b>.</li> <li>b. <b>SEC_LOCK</b>: Contact the employee's manager to determine the current status of the employee.</li> <li>c. <b>SLF_LOCK</b>: (<b>LOKME</b>) Review and verify with manager the dates or time-frame the Self-Lock was set.</li> </ol> </li> </ol>

**Exhibit 4.2.9-2 (07-06-2020)****Sensitive Access (Other/Spouse) Report**

This report must be certified within 14 calendar days after the report date for the certification to be considered timely. This report identifies users who have attempted to or who have accessed other employees' or the spouses/ex-spouse of other employees' accounts. Before this report can be certified, each Social Security Number (SSN) on this report must be researched to determine if the access to other IRS employees' accounts and/or their spouses' accounts, was business related.

Validate that the access is supported by one of the following:

- Direct case assignment.
- Related case assignment.
- Evidence of cross compliance checks.
- Department of Justice or other official requests.
- Confirmed input error supported by the identification of another assigned case with similar Taxpayer Identification Number (TIN), such as a transposition or formatting error.
- A detailed justification statement from the manager when the group or certain employees work assignments will generate reoccurring accesses on this report.

When there is no direct case assignment, but the case is controlled on ERCS, the USR shall validate the access.

If further research is required to validate the access, then the USR shall use research and analytical tools to:

<b>Action:</b>	<b>Then:</b>
Determine if the account is controlled on Exam Return Control System (ERCS)	Document findings on IORS.
Determine if Form 11377, Taxpayer Data Access, was submitted	Document findings on IORS.
E-mail the accessing employee's manager to validate the access. The e-mail to the manager must include: <ul style="list-style-type: none"> <li>• Specific information to identify the user.</li> <li>• The date and time stamp of the access.</li> <li>• The account accessed.</li> <li>• The command codes accessed.</li> </ul>	Document findings on IORS.
If manager is unable to validate the access, the USR shall initiate an Audit Trail via Form 9936, Request for Audit Trail Extract	Document findings on IORS.
If the audit trail does not validate the access	the USR must coordinate with the manager and refer the potential UNAX violation to TIGTA.

**Exhibit 4.2.9-3 (07-06-2020)**  
**Monthly IDRS Security Profile Report**

Unit managers and USRs are responsible for:

- The review of this report to help detect unauthorized user activity or problems with IDRS.
- Referring any indication of illegal or improper activity to the proper management staff or TIGTA.
- Ensuring that this report is thoroughly reviewed monthly, and the following actions below are taken:

<b>Action:</b>	<b>Resolution:</b>
Review the command code usage by unit	Submit Form 9937 via IORS to EOPs, Security Account Administrators to delete the command codes that are not used or no longer needed in the MPAF.
Report any suspicious activities timely to TIGTA	Questionable activities or potential UNAX violations are scrutinized.
Review the role restrictions on IDRS user's profiles	All users who meet the criteria for a restricted profile have the appropriate restriction(s) placed against their profile with CC RSTRK Definer A or CC RSTRK Definer R, whichever is appropriate.
Identify locked employee profiles or no command code activity	Coordinate with manager to determine if employee should be deleted from IDRS.
Review Inactivity SINOF	Advise users who have 15 or more automatic sign-offs for the month to sign off IDRS when not needed. Ensure users are aware of how to refresh their IDRS activity clock using CC RFRSH if the user needs to have continuous access to IDRS.

**Exhibit 4.2.9-4 (07-06-2020)**  
**Report Level Actions**

<b>Assigned Report Level Action:</b>	<b>Report Level Comments:</b>	<b>Current Certification Status:</b>
<ul style="list-style-type: none"> <li>• Review/Validated- No Follow-up Action Needed</li> <li>• Follow-up Action Needed</li> <li>• Follow-up Action Completed</li> <li>• Referred to AWSS/TIGTA</li> <li>• Other (Comment Required)</li> </ul>	N/A	<ul style="list-style-type: none"> <li>• Report Certified</li> <li>• Remove Certification/Not Certifying</li> </ul>
<p><b>Action:</b> Use drop-down arrow to select one of the above actions</p>	<p><b>Action:</b> The USR will use this section to summarize actions taken that commanded follow-ups, UNAX referral, or any questionable event that required escalation to the appropriate authorities.</p>	<p><b>Action:</b> The USR must certify the report and has the option to remove the certification and re-certify if warranted.</p>



