EFFECTIVE DATE

(10-16-2023)

PURPOSE

(1) This transmits revised IRM 5.1.25, Field Collecting Procedures, IDRS and Data Security for Collection.

MATERIAL CHANGES

(1) IRM 5.1.25, Audience: Updated Director's Name and Title

(2) IRM 5.1.25.1.1(2), Background: Modified IRM reference to IRM 10.8.34.2.1.3.

(3) IRM 5.1.25.1.3(1), Responsibilities: Modified IRM reference to IRM 1.1.16.3.3.3.2.

(4) IRM 5.1.25.1.6(1), Terms and Acronyms: Added Acronyms BEARS and SAA with definitions.

(5) IRM 5.1.25.1.7(2), Website References: Updated website links for Collection Automation Support & Security(CASS) Share Point site and Taxpayer Data Access Library.

(6) IRM 5.1.25.2, IDRS Security Personnel: Updated IRM reference to IRM 10.8.34.2.

(7) IRM 5.1.25.2.1(2)b), Managers of IDRS Users: Added Night shift procedures for Campus Function managers.

(8) IRM 5.1.25.2.1(2)c), Managers of IDRS Users: .Added request to be designated as a Terminal Security Administrator.

(9) IRM 5.1.25.2.1(2)d), Managers of IDRS Users: Added designate a bargaining unit employee (e.g., Lead) to be an Alternate USR.

(10) IRM 5.1.25.2.2(2)b), Data Security Analyst (DSA): Updated to clarify DSA's response to Group Manager and/or both Primary Manager/Sharing Manager of Shared Administrative Associate(SAA) for command code requests.

(11) IRM 5.1.25.2.2 (2)i), Data Security Analyst: Updated OL5081 request to BEARS entitlement.

(12) IRM 5.1.25.2.3(1),IDRS User Support: Updated centralized mailbox time to 5:00p.m..

(13) IRM 5.1.25.3.2 (1), IDRS Command Codes, Updated sentence structure to make two statements.

(14) IRM 5.1.25.3(3), IDRS User Support: Added Non-PIV IDRS SINON as part of IDRS profile locks criteria.

(15) IRM 5.1.25.3(3), IDRS User Support: Updated the table by adding new requirement under Notes: the title of the Manager or Acting Manager must be in the body of the e-mail or the signature line.

(16) IRM 5.1.25.3(4), IDRS User Support: Updated OL5081 to a BEARS entitlement request.

(17) IRM 5.1.25.3(4), IDRS User Support, Request New Application (Add User):) Updated Add Access BEARS entitlement procedures for IDRS application appropriate SB/SE assignment.

(18) IRM 5.1.25.3(4), IDRS User Support, Request New Application (Add User) Updated Add Access BEARS entitlement procedures for provisioning and Shared Administrative Associate requirements on BEARS entitlements.

(19) IRM 5.1.25.3(4), IDRS User Support, (Request New Password) Updated OL5081 to a BEARS entitlement.

(20) IRM 5.1.25.3(4), IDRS User Support, (Modify User profile for Legal or Pseudonym name change): Updated OL5081 to BEARS entitlement and added Access BEARS entitlement.

(21) IRM 5.1.25.3(4), IDRS User Support, (Modify User profile Add/delete security command codes) Updated to clarify DSA submission procedures for Form 13230. Added EOPS requirement for additional Fom 13230 specified permissions. Updated and Added procedures for removing security command codes and former designee.

(22) IRM 5.1.25.3(4) , IDRS User Support, (Delete account/Delete User) Updated OL5081 delete request to Remove Access Bears entitlement request, Added EOPS process for daily application deletions.

(23) IRM 5.1.25.3.1(c), IDRS Unit Profiles, Added Shared Administrative Associates(SAA) units process for approved command codes to the MPAF profile.

(24) IRM 5.1.25.3.2(3), IDRS Command Codes: Added managerial approval to update the unit or employee profiles.

(25) IRM 5.1.25.3.2.2(1)1)., Requests for Uncommon Command Codes: Added verification process for user with 809 restriction.

(26) IRM 5.1.25.3.2.2(1)3), Request for Uncommon Command Codes, For Field Revenue Officer: Added DSA procedures for Non-809 receipt book holder Revenue Officers profiles.

(27) IRM 5.1.25.3.2.2(1)3), Request for Uncommon Command Codes,: Added procedural guidance for Shared Administrative Associate.

(28) .

(29) IRM 5.1.25.4.1.3.1(1), Weekly Security Violations Report: Added Excessive Use (PWMGT).

(30) IRM 5.1.25.4.1.3.1(3)a), Weekly Security Violations Report: Added Excessive use to table and DSA reviewing procedures for violation.

(31) IRM 5.1.25.4.1.3.1(3)c), Weekly Security Violations Report: If: Added 21 day Non-PIV IDRS SINON Usage lock Then: Added DSA procedures to address PIV card for IDRS.

(32) IRM 5.1.25.4.1.3.2(6), Weekly Sensitive Access (Other/Spouse): Updated Note for Box 10 of Form 11377 or Form 11377-E.

(33) IRM 5.1.25.4.1.3.2(8)(9), Weekly Sensitive Access (Other/Spouse): Added certification statement for SAA accesses and moved DSA requests a response statement within 5 business days to (9).

(34) IRM 5.1.25.4.1.3.2.(9), Weekly Sensitive Access (Other/Spouse): Added statements to If and Then table for SAA employee access and Updated IRM reference to 10.8.34.2.2.8(9)h.

(35) IRM 5.1.25.5(1)c), Monthly IDRS Security Profile Report, Locked Profiles: Added 21 day Non-PIV IDRS SINON Then: Added DSA guidance for PIV installation and assistance with SMART card Pin.

(36) IRM 5.1.25.5(2)b)c), Monthly IDRS Security Profile Report, Locked Profiles: Updated DSA procedures on Remove Access BEARS entitlement and. (c) Updated to remove OL5081 and added EOPS daily BEARS process.

(37) IRM 5.1.25.5.2(3), Automated Command Code Access Control / Restrictions: Updated IRM reference to IRM 10.8.34.5.2.1.6.8.

(38) IRM 5.1.25.5.4(b), Security Command Code Usage: Updated to Modify Access BEARS entitlement.

(39) IRM 5.1.25.5.6(7), Security Audit and Analysis System (SAAS): Updated IRM . reference to 10.8.34.2.2.8(9)h.

(40) IRM 5.1.25.7(1)3), Form 11377 / 11377-E, Taxpayer Data Access: .Added Note statement for SAA employee on submission process Form 11377-e.

(41) IRM Exhibit 5.1.25-1, Acronyms: Added acronym BEARS, Business Entitlement Access Request System, EOPS, Enterprise Operations, HOD, Head of Office Designee, SAA Shared Administrative Associate and Removed OL5081.

(42) IRM Exhibit 5.1.25-2, Command Codes - SB/SE Collection Operations and Operations Support: Updated table titles and formatting. Added table and title for SAA approved command codes and header rows for all tables.

(43) Editorial changes were made throughout the IRM to clarify language, correct typographical errors and formatting, and to update/add links, website addresses and/or titles.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 5.1.25 dated June 8, 2020.

AUDIENCE

Small Business/Self-Employed, Collection Operations and SB/SE Operation Support Employees.

Nikki C. Johnson
Director, Headquarters Collection
Small Business/Self Employed

5.1.25
IDRS and Data Security for Collection

Table of Contents

Exhibits

5.1.25.1
(06-08-2020)
Program Scope and Objectives

(1) ***Purpose:*** This IRM section provides policies and guidance to carry out 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), Collection Operations managers, Operation Support managers and the IDRS Data Security group. The audience includes:

Organization	Offices
Collection Operations	• Civil Enforcement, Advice and Support Operations • Field Collection • Headquarters Collection • Planning and Performance Analysis • Specialty Collection - Insolvency • Specialty Collection - Offer in Compromise
Operations Support	• Business Development • Business Support • SB/SE Human Capital • Technology Solutions

(3) **Policy Owner:** The Director, Collection Operations - Headquarters Collection - Quality and Technical Support is responsible for issuing policy.

(4) **Program Owner:** The program owner is the IDRS Data Security Group, under Collection Automation Support & Security (CASS), an organization within SB/SE – Quality and Technical Support.

(5) **Primary Stakeholders:** The primary stakeholders are SB/SE Collection Operations and Operations Support.

(6) **Program Goals:** The primary goal of this IRM is to provide procedural guidance, ensuring consistency with the work product. This includes the timely review and certification of security reports along with addressing user support inquiries, not detailed in another IRM.

5.1.25.1.1
(10-16-2023)
Background

(1) IRM 5.1.25, IDRS and Data Security for Collection, 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.

(2) The IRM 10.8.34.2.1.3, 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. SB/SE Collection Operations and Operations Support established dedicated Unit Security Representatives (USRs), known by their organizational title as Data Security Analysts (DSAs).

(3) DSAs are responsible for ensuring all aspects of data security are followed and coordinate with the Group Manager where issues arise.

5.1.25.1.2
(08-02-2019)
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 Part 10 takes precedence over this IRM unless requirements within this IRM are more stringent.

5.1.25.1.3
(10-16-2023)
Responsibilities

(1) The IDRS Data Security Group is assigned to the CASS function. DSAs in Collection perform the security duties, which in other functions fall to managers of IDRS users. See IRM 1.1.16.3.3.3.2, Collection Automation Support & Security, for information on the role and mission of the CASS function.

(2) IRM 5.1.25.2, IDRS Security Personnel, further defines the roles of the Group Manager, DSA, Alternate DSA, and Terminal Security Administrator (TSA).

5.1.25.1.4
(06-08-2020)
Program Management and Review

(1) SB/SE Collection IDRS Data Security Manager:

a. monitors and reviews 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. collaborates with SB/SE Collection Operations, Operations Support and IT Cybersecurity personnel to address emerging issues.

(2) CASS Program Manager conducts annual operational reviews following general guidelines in IRM 1.4.50, Collection Group Manager, Territory Manager and Area Director Operational Aid.

5.1.25.1.5
(08-02-2019)
Program Controls

(1) The IORS application maintains a record of all certifications by the Primary Report Reviewer for each report requiring certification and for each IDRS unit under their responsibility.

(2) Business organizations shall achieve at least a 90% certification rate for their security reports.

(3) Cybersecurity IDRS Security analysts:

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 list of uncertified reports.
c. work with business organizations in their campus domain(s) to address IDRS security report certification related issues.
d. advise business organizations in their campus domain(s) of any units where a Primary Report Reviewer has not been designated.

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

5.1.25.1.6
(10-16-2023)
Terms and Acronyms

(1) This IRM section contains the following terms:

Term	Definition
Audit Trail	A chronological record of transactions entered on IDRS or related applications.
BEARS	The BEARS application is a means to request and document user access to systems/ applications. Users access the BEARS application via a website on the IRS Intranet. BEARS has a user base of 100,000 + nationwide and does not collect taxpayer information. BEARS replaced the OL5081 application.
Campus	A centralized Internal Revenue Service processing site.
Certification	Refers to the process by which an IDRS user's sensitive accesses and security violations have been verified as appropriate or addressed.
Command Codes	A five-character terminal input on IDRS to extract a specific set of data or used to input an action.
IDRS	Integrated Data Retrieval System – a computer system with the capability to obtain or update information on taxpayer accounts.
Shared Administrative Associate	The Shared Administrative Associate (SAA) position provides administrative, clerical and case processing support to managers and technical employees with the ability to utilize IDRS cross-functionally throughout assigned organizations.
Timely	In accordance with established due dates.

(2) A list of commonly used acronyms and their definitions are in IRM Exhibit 5.1.25-1.

(3) Additional acceptable acronyms and abbreviations are in ReferenceNet at: *Acronyms Database (irs.gov)*

5.1.25.1.7
(10-16-2023)
Related Resources

(1) IRM References:

- IRM 2.3, IDRS Terminal Responses
- IRM 2.4, IDRS Terminal Input

(2) Website References:

- CFOL (Corporate Files On-Line) Express: *http://serp.enterprise.irs.gov/databases/job-aids/misc/cfol-express.pdf*
- Collection Automation Support & Security (CASS) SharePoint site: *CASS Employee SharePoint Site*
- Document 6209, IRS Processing Codes and Information: *http://serp.enterprise.irs.gov/databases/irm.dr/current/6209/6209.html*
- IDRS Command Code Job Aid: *http://serp.enterprise.irs.gov/job-aids/command-code/command-code.html*
- IDRS Online Report Services (IORS): *Overview - IORS (irs.gov)*
- IDRS Unit and USR Database (IUUD): *IUUD - IORS (irs.gov)*
- SB/SE Collection IDRS Data Security Contact List: *http://serp.enterprise.irs.gov/databases/who-where.dr/idrs-data-security.html*
- Taxpayer Bill of Rights: *Taxpayer Bill of Rights | Internal Revenue Service (irs.gov)*
- Taxpayer Data Access Library: *SBSE Service Center and Collection (sharepoint.com)*

5.1.25.2
(10-16-2023)
IDRS Security Personnel

(1) This section provides supplemental roles and responsibilities for personnel who have IDRS security-related responsibilities. These roles are further defined in IRM 10.8.34.2, Roles and Responsibilities.

5.1.25.2.1
(10-16-2023)
Managers of IDRS Users

(1) SB/SE Collection Operations and Operations Support Managers:

a. coordinate with the DSA to ensure IDRS security is effectively implemented for the unit/group.
b. advise the DSA when a user is transferred in or out of the workgroup.
c. arrange periodic IDRS and Data Security awareness presentations for the workgroup. Contact your assigned DSA for a group presentation.
d. ensure the DSA is notified immediately when an IDRS user no longer requires system access.
e. respond within five business days to the DSA with findings related to questionable accesses and/or other security report inquiries.

(2) SB/SE Collection Operations and Operations Support Managers may:

a. request secondary permissions in IORS to view, add comments, and/or print their own unit reports.
b. Night shift Campus Function managers **only** can request to be designated as an Alternate USR with appropriate BEARS entitlement for specified command codes.
c. request to be designated as a Terminal Security Administrator
d. designate a bargaining unit employee (e.g. Lead) to be an Alternate USR. However, a bargaining unit Alternate USR is not allowed to review another employee's IDRS actions.

Note: This designation does not impact the roles and responsibilities of the DSA.

5.1.25.2.2
(10-16-2023)
Data Security Analyst (DSA)

(1) The DSA:

a. is listed as the IORS Primary Reviewer and the Primary USR on the IDRS Unit and USR Database (IUUD) for their assigned IDRS units.
b. is assigned a range of IDRS unit numbers aligned within SB/SE Collection Operations and Operations Support areas.
c. maintains an active IDRS profile on both the Enterprise Computing Center - Martinsburg (ECC-MTB) and Enterprise Computing Center - Memphis (ECC-MEM) to ensure unrestricted backup support.
d. is profiled with ALLOW permissions to support users on all SB/SE home campuses.
e. is responsible for the review and certification of IORS and Security Audit and Analysis System (SAAS) reports.

(2) The DSA also performs the following unit and account administration related tasks:

a. Support the program goals of IT Cybersecurity by providing assistance, analysis and recommendations for action to SB/SE Collection Operations and Operations Support management.
b. Responds to Group Manager or both Primary Manager/Sharing Manager of Shared Administrative Associate(SAA) request to add or delete command codes sent directly to DSA or the centralized mailbox (*SBSE CASS IDRS Security).
c. Request new IDRS command codes for the unit profile using Form 9937, IDRS Unit Request
d. Respond to user requests to unlock IDRS profiles and terminals.
e. Support related functions, such as the IDRS Password Management Capability and the Integrated Automation Technologies (IAT) tool bar
f. Maintain a centralized storage of Form 11377 and Form 11377-E, Taxpayer Data Access for each SB/SE Collection Operations and Operations Support area.
g. Use IORS to monitor IDRS usage and security.
h. Use Security Audit and Analysis System (SAAS) to monitor accesses to the Transcript Delivery System (TDS) and Modernized e-File Return Request & Display (MeF-RRD).
i. Approve BEARS entitlements to add, delete or modify IDRS user profiles.
j. Coordinate with other CASS functions to support reorganizations through the SB/SE Request for Organizational Change process.
k. Submit updates to the IUUD to reflect current managerial contact information.

5.1.25.2.3
(06-08-2020)
Alternate Data Security Analyst (DSA)

(1) At CASS management's discretion, a cadre of Alternate DSAs perform the role of the Primary DSA as a collateral duty. Additionally, they:

a. are non-bargaining unit employees.
b. maintain active profiles on the ECC-MTB and ECC-MEM.
c. are profiled with ALLOW permissions to support users on all SB/SE home campuses.

5.1.25.2.4
(08-02-2019)
Terminal Security Administrator (TSA)

(1) A Terminal Security Administrator (TSA) is designated by area management to provide additional IDRS user support in unlocking IDRS user profiles and terminals only. TSAs are bargaining unit or non-bargaining unit employees.

5.1.25.3
(10-16-2023)
IDRS User Support

(1) IDRS users or their managers are encouraged to submit all requests to a centralized mailbox at **SBSE CASS IDRS Security*. The mailbox is generally staffed from 6:00 a.m. to 5:00 p.m. (Central Standard Time) Monday through Friday.

(2) Routine requests submitted by e-mail are generally completed within thirty minutes of receipt, except where final approval is required by the Campus IDRS Security Analyst.

(3) Upon receipt of an e-mail request from an IDRS user or manager, the DSA is responsible for providing IDRS user support as follows:

(4) The actions requested below require the IDRS user or manager to submit a BEARS entitlement request.

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

5.1.25.3.1
(10-16-2023)
IDRS Unit Profiles

5.1.25.3.2
(10-16-2023)
IDRS Command Codes

5.1.25.3.2.1
(06-08-2020)
Requests for Common Command Codes

5.1.25.3.2.2
(10-16-2023)
Requests for Uncommon Command Codes

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

5.1.25.4
(08-02-2019)
IDRS Online Reports Services (IORS)

(1) IORS is a web based application that makes IDRS security reports available online to IDRS security staffs and authorized business reviewers.

(2) The DSA is designated as the IORS Primary Reviewer for all Collection Operations and Operations Support IDRS units.

(3) Managers of IDRS users may be granted secondary permissions in IORS to view, add comments, and print IORS reports for their assigned unit.

5.1.25.4.1
(08-24-2016)
Types of IORS Reports

(1) There are four weekly security reports available to authorized users for review and necessary actions.

- Employee Count by Site/Unit
- Master Register of Active IDRS Users
- Security Violations
- Sensitive Access (Other/Spouse)

(2) There are three monthly reports available to authorized users for review and necessary actions.

- Automated IDRS Sign-Offs Due to User Inactivity
- Monthly IDRS Security Profile Report
- Password Management Activations

5.1.25.4.1.1
(12-11-2014)
Weekly Security Reports - Review and Action (No Certification Required)

(1) The Employee Count by Site/Unit report lists the number of active users in each unit. The DSA reviews this report and take action as warranted, such as deleting empty units that are no longer required to support the area footprint.

(2) The Master Register of Active IDRS Users report lists numerous fields of information for all active users in the unit. The DSA incorporates the Master Register of Active IDRS Users report in their monthly security review activities.

5.1.25.4.1.2
(06-08-2020)
Monthly Security Reports - Review and Action (No Certification Required)

(1) The Automated IDRS Sign-Offs Due to User Inactivity report lists those users whose IDRS sessions terminated after 120 minutes of inactivity. The DSA takes the following action:

a. Identify IDRS users with more than 15 automatic sign-offs in a month.
b. Advise those users to sign-off IDRS when not in use to prevent an unauthorized access.
c. Instruct users how to periodically refresh their IDRS session if IDRS is required on a continuous basis.

Note: While this report is not certified independently, it is incorporated as an aspect of certifying the Monthly IDRS Security Profile Report.

(2) The Password Management Activations 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 DSA researches to determine if IDRS Password Management has been activated since the report was generated.

- If yes, no further action is warranted.
- If no, the DSA sends an e-mail to the user with a copy to the manager requesting the user to activate the IDRS Password Management capability. The DSA attaches the instructions to assist the user with activation.

Note: While this report is not certified independently, it is incorporated as an aspect of certifying the Monthly IDRS Security Profile Report.

5.1.25.4.1.3
(08-24-2016)
Security Reports Requiring Certification

(1) The DSA is required to review and certify the following security reports:

- Weekly Security Violations Report
- Weekly Sensitive Access (Other/Spouse)
- Monthly IDRS Security Profile Report

5.1.25.4.1.3.1
(10-16-2023)
Weekly Security Violations Report

(1) This report lists all security violations recorded by IDRS users, such as:

- Password Mismatch
- Name Mismatch
- SINON Error (PWMGT)
- Response Error (PWMGT)
- Command Code Not in Profile
- Locked Profile
- Excessive Use (PWMGT)

(2) Timely certification is within 14 calendar days after the end date for the period.

(3) The DSA is required to complete the research and take appropriate actions as follows:

a. The report reflects a user with SINON violations.

If	Then
The research shows a user has four or more violations with any combination of: • Password Mismatch • Name Mismatch	(1) Send an e-mail to the user, with a courtesy copy (cc:) to the manager to confirm the following: • The user committed these errors • The violations were not the result of an unauthorized attempt to access IDRS. ***Note:*** If the user contacted a DSA or the IDRS centralized mailbox, an e-mail is not required. (2) Advise Treasury Inspector General for Tax Administration (TIGTA) of the user's response if the user does not agree they committed the violations.
The research shows a user has one or more IDRS Password Management violations such as: • SINON Error • Response Error • Incomplete • Excessive Use	Send an e-mail to the user, with a courtesy copy (cc:) to the manager with instructions on how to reset IDRS Password Management. ***Note:*** **Excessive** Use Send an email to the user with a courtesy copy(cc:) to the manager to advise employee cannot use Password Management capability successfully more than five times within a 30-day period. If employee has exceeded their usage limit and needs a password submit a Password Reset BEARS entitlement.

b. The report reflects a user with four or more Command Code Not in Profile violations. Research the user's profile to determine if the command code(s) were previously added.

If	Then
Command Codes(s) were previously added	No further action is required

If	Then
Command Code(s) were not previously added.	(1) Determine if the command code(s) is authorized for SB/SE Collection Operations and Operations Support function and position use (Refer to IRM 5.1.25.3.2, IDRS Command Codes). (2) If authorized, e-mail the user with a cc: to the manager stating: • The command code(s) accessed resulted in a security violation. • If the command code is needed for their position, to obtain managerial approval to have the command code added to their profile. ***Note:*** If not needed or it was an input error, no further action is required. (3) If not authorized, e-mail the user, with a courtesy copy (cc:) to the manager, advising the command code is restricted and/or not allowed in SB/SE Collection Operations and Operations Support profiles.

c. The report shows a user with a Locked Profile violation. Research the user's profile to determine the current status.

Example: System Lock due to inactivity, Security Lock, or the employee initiated a Self-Lock.

If	Then
The IDRS profile is unlocked	No further action is required.
A System Inactivity Lock exists	The manager determines if account is unlocked or remains locked.
A 21 Day Non-PIV IDRS SINON Usage Lock	The DSA determines if employee has an active PIV card and assists with SACS/IDRS PIV Authentication installation. The DSA provides guidance with instructions to sign on IDRS using their SMART card Pin.
A Security Lock exists	Contact the manager to request the current status of the user.

If	Then
A Self-Lock was initiated	Review the dates the Self-Lock was set and date the violation occurred. On a case-by-case basis, the DSA contacts the manager to determine if the employee is out of the office for the period in question.

(4) The DSA documents IORS for every actionable event.

(5) In the comments area, the DSA documents all research, contacts made with the user or manager, and their conclusion.

(6) For each individual action taken, the DSA selects the appropriate action for the event from the drop-down menu:

- Review Completed - No Follow-up Needed
- Review Completed - Follow-up Performed
- Follow-up Action Required
- Other (Comment Required)

(7) The DSA addresses Report Level Actions, Report Level Comments and Current Certification Status, which apply to all displayed units.

Report Level Items	Actions
Report Level Actions	• Reviewed and Validated - No Follow-up Action Needed • Follow-up Action Needed • Follow-up Action Completed • Referred to AWSS or TIGTA • Other (Comment Required)
Report Level Comments	• The DSA summarizes actions taken to review the Weekly report.
Current Certification Status	• Report Certified • Remove Certification / Not Certifying

5.1.25.4.1.3.2
(10-16-2023)
Weekly Sensitive Access (Other/Spouse)

(1) This report lists users who attempted or accessed other employees' or the spouses/ex-spouse of other employees' accounts.

(2) The DSA is required to review each unique Social Security Number (SSN) to ensure all accesses to other Internal Revenue Service (IRS) employees' and/or their spouses' accounts are business-related.

(3) Accesses are supported by one of the following:

Note: Prior certifications are found by clicking the "View All Accesses by User to Same SSN Within 12 Months" link.

a. Direct case assignment in SB/SE Collection inventory applications, such as the Integrated Collection System (ICS), Automated Insolvency System (AIS), or Automated Offers in Compromise (AOIC).
b. Related case assignment on SB/SE Collection inventory applications.
c. Evidence of cross compliance checks.
d. Department of Justice or other official requests.
e. Confirmed input error supported by the identification of another assigned case with similar Taxpayer Identification Number (TIN), such as a transposition or formatting error.

(4) The DSA is required to certify all accesses through collection case assignment by querying the SSN on SB/SE Collection inventory applications. When the accessing user is assigned the case or is another member of the same group the DSA certifies the access.

Note: The DSA leaves a history on ICS identifying the purpose of the access.

(5) Timely certification is within 14 calendar days after the end date for the period.

(6) The DSA takes the action shown in the following table if unable to certify the access:

If	**Then**
No record is located on the inventory applications	Research Form 11377s on the Taxpayer Data Access Library.
A document exists with sufficient explanation	Certify the access.
No document exists	Research IDRS and/or other applications, such as Accounts Management Services (AMS) to locate a cross-reference TIN.
A cross-reference TIN is located	Research inventory applications to determine whether the related TIN controls case assignment.

Note: The DSA prepares Form 11377 or Form 11377-E for all IDRS accesses of employee/spouse accounts to include in Box 10:

- Which Campus report researched
- IORS week XX
- Reason for the Access
- Submit the form to the SB/SE Collection IDRS Data Security Manager.

(7) If the research performed above does not confirm or certify the access the DSA emails the manager of the accessing user to validate the access.

(8) If the research above does not confirm or certify SAA accesses, the DSA emails the primary manager and sharing manager of the SAA employee.

(9) The DSA requests a response within five business days and includes the following in the e-mail:

- Specific information to identify the user
- The date and time stamp of the access
- The account accessed
- The command codes accessed
- The DSA's research

Note: Based on the e-mail response, the DSA takes the following action:

If	Then
Response from: • The manager provides a valid reason for the access. • The primary manager and/or sharing manager provide a valid reason for the SAA employee access.	The DSA conducts additional research to confirm a related case assignment. ***Example:*** If the response states the access is a cross compliance check to a business entity or a transposition error, the DSA independently confirms the actual case assignment. ***Exception:*** Centralized Campus Operations receive recorded phone calls, which are retained and reviewed locally, for up to 30 days after the contact. ***Example:*** If the response shows the relationship between the questionable access and the TIN assigned to the employee, trainee, or group.
The manager cannot provide a valid reason for the access	The DSA initiates Form 9936, Request for Audit Trail Extract, to view what actions were recorded before and after the access in question. ***Note:*** If a manager requires an IDRS audit trail for any reason not associated with a security report, they request it through the DSA or by direct contact with IT Cybersecurity.

If	Then
The manager has not replied within five business days	The DSA sends a copy of the initial e-mail to the Territory Manager with a cc: to the Group Manager.
The DSA does not receive a response within an additional five business days	The DSA notifies the SB/SE Collection IDRS Data Security Manager.
The DSA cannot certify an access through independent research, managerial response and/or reviewing audit trails	The DSA submits a referral to TIGTA for follow up in accordance with IRM 10.8.34.2.2.8(9)h, Security Reports Requiring Certification by a Primary Report Reviewer.

(10) In the comments area on IORS, the DSA clearly and concisely documents all research conducted and actions taken. This includes research results and any contacts with the user and/or manager. The comments provide enough detail to enable any reviewer to understand how the DSA certified the access or why it was referred to TIGTA.

Note: If a TIGTA referral is required, the DSA certifies the report and subsequently records the complaint number upon receipt.

(11) For each unique SSN, the DSA selects the appropriate action for the event from the drop-down menu:

- Review Completed - No Follow-up Needed
- Review Completed - Follow-up Performed
- Follow-up Action Required
- Other (Comment Required)

(12) The DSA addresses Assign Report Level Items, Report Level Comments and Current Certification Status, which apply to all displayed units as shown in IRM 5.1.25.4.1.3.1(7).

Note: If the DSA sets the Assign Report Level Action to “Follow-up Action Needed,” and the Current Certification Status to “Remove Certification / Not Certifying”, they ensure the report is monitored through certification.

5.1.25.5
(06-08-2020)
Monthly IDRS Security Profile Report

(1) The Monthly Security Profile Report provides a summary of various IDRS security aspects. Every unit is reviewed for the following categories:

- Locked Profiles
- Automated Command Code Access Control/ Restrictions
- Sensitive Command Code Combinations
- Security Command Code Usage
- Master Register of Active IDRS Users
- Command Code Activity

(2) Timely certification is within 28 calendar days after the end date for the period.

5.1.25.5.1
(10-16-2023)
Locked Profiles

(1) The DSA reviews locked IDRS profiles of 28 days or more due to inactivity. Research IDRS to determine if the user has been deleted from IDRS or if the profile is still locked.

a. If the user profile has since been unlocked or deleted, no further action is required.
b. If the user profile is still locked, the DSA sends an e-mail to the manager to determine if the user still requires IDRS access.
c. If the user profile has a 21 Day Non-PIV IDRS SINON usage lock. The DSA determines if the employee has an active PIV card and assists with SAC/ IDRS PIV Authentication installation. The DSA provides guidance with instructions to sign on IDRS using SMART card Pin.

(2) Based on the manager's response, the DSA performs the following action:

a. If the manager confirms the user requires IDRS access, the user is unlocked upon request.
b. If the manager determines the user no longer requires IDRS access, the DSA advise manager to initiate a Remove Access BEARS entitlement. If expedited treatment is required, the manager contacts the DSA who manually deletes the user from IDRS.
c. Enterprise Operations(EOPS) process BEARS Others entitlements daily to remove requested active IDRS applications.

5.1.25.5.2
(10-16-2023)
Automated Command Code Access Control / Restrictions

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#
#

#
#

5.1.25.5.3
(08-02-2019)
Sensitive Command Code Combinations

(1) SB/SE Collection Operations and Operations Support IDRS units may contain sensitive command code combinations, which require increased oversight. See IRM Exhibit 10.8.34-6, Sensitive Command Code Combinations, for the list of codes.

(2) The DSA ensures the UCCP does not contain any sensitive command code combinations.

(3) The DSA sends the Sensitive Command Code Combination reports to the manager for monitoring.

5.1.25.5.4
(10-16-2023)
Security Command Code Usage

(1) The DSA queries their units to identify the use of security command codes to ensure they are apprised of all users approved by local management to function as Alternate USRs or TSAs.

(2) If security command codes have not been used for over six months, contact the user's manager to confirm the user's security role. Based on the manager's response, perform the following actions:

a. If the manager concurs with the user's continued security role, no further action is required.
b. If the manager determines the user no longer requires security command codes, direct the manager to initiate a Modify Access BEARS entitlement request to delete the user's security command codes.

Exception: The Centralized Campus Operations are exempt as each Group Manager and/or Lead typically has access to their own unit and/or work second shift when no other coverage is available.

5.1.25.5.5
(08-02-2019)
Master Register of Active IDRS Users

(1) The Master Register lists active IDRS users in the unit.

(2) The DSA validates each workgroup's Master Register in any way they deem appropriate to identify discrepancies.

(3) The DSA is responsible for taking any corrective actions necessary, such as: moving the user to another unit, updating the user's phone number in IDRS and confirming approved pseudonym names are reflected in IDRS.

5.1.25.5.6
(08-24-2016)
Command Code Activity

(1) The DSA reviews unit and individual command code usage to determine:

a. if the MPAF command codes are appropriate for the work performed by the users in the unit.
b. whether UCCP command codes are used by at least 90 percent of IDRS users in the unit. The UCCP shall not contain any sensitive command codes unless 100 percent of the employees in the unit need the command code to do their work.

(2) The DSA reviews the profile of each IDRS user to identify any unauthorized command codes. See Exhibit 5.1.25-2 for a list of common MPAF production command codes approved for use by SB/SE Collection Operations and Operations Support.

(3) Based on results of the unit and individual command code review, take the following action, if appropriate:

a. Request the IDRS Security Account Administrator modify or delete the command codes that are not authorized, used, or no longer needed in the MPAF or UCCP
b. Review users with command code REPTS in their profile, especially users in IORS specific units, to determine if IORS access is still needed

Exception: The Centralized Campus Operations are exempt as each Group Manager and/or Lead typically has access to their own unit and/or work second shift when no other coverage is available.

c. Report questionable patterns of command code activities to the manager.

5.1.25.5.7
(08-02-2019)
IORS Documentation

(1) The DSA enters comments at the Report Level Items, as the Monthly Security Profile Report is certified in its entirety.

(2) The DSA summarizes actions taken to address each security aspect. The monthly review includes the entire area or a specific unit range.

(3) The DSA addresses all Report Level Items, Report Level Comments and Current Certification Status which apply to all displayed units as shown in IRM 5.1.25.4.1.3.1(7).

5.1.25.6
(10-16-2023)
Security Audit and Analysis System (SAAS)

(1) Audit trails for modernized applications are stored in the SAAS.

(2) In compliance with each application's audit plan, business units are responsible for reviewing SAAS audit trails and certifying accesses to taxpayer data.

(3) The IDRS Data Security Group currently monitors the audit trail extracts for access to TDS and MeF-RRD. Security reviews in SAAS may be expanded at any time to include additional applications.

(4) For each application there is a General Access and Access to Employee report. The General Access report is subject to a sample review and certification. The business unit determines the sample percentage, which is subject to change. The Access to Employee report is subject to 100% review and certification.

(5) The DSA generally certifies the sample reports within 14 calendar days of receipt. CASS management approves longer certification due dates, as appropriate.

(6) The DSA follows the established certification procedures by attempting to confirm case/related case assignment in SB/SE Collection Operations and Operations Support inventory applications. If case assignment is not independently confirmed, the DSA contacts the manager to justify the access.

(7) If the DSA is unable to certify an access through independent research or managerial response, the DSA submits a referral to TIGTA for follow-up in accordance with IRM 10.8.34.2.2.8(9)h.

(8) Unlike IORS, SAAS does not have the capability to capture review comments. The review notes documented by the DSA are maintained by the SB/SE Collection IDRS Data Security Manager for 90 days. Certification results are submitted to IT Cybersecurity as directed.

5.1.25.7
(10-16-2023)
Form 11377 / 11377-E, Taxpayer Data Access

(1) The purpose of Form 11377 or Form 11377-E, Taxpayer Data Access, is to provide employees with a method to document accesses to taxpayer return information, when the accesses:

a. are not supported by direct case assignments.
b. are performed in error.
c. may raise suspicion.

(2) Use of Form 11377 or Form 11377-E is voluntary.

(3) If the employee completes the Form 11377 or Form 11377-E, the manager forwards the IRS copy to the designated Head of Office Designee (HOD) by close of business or as soon as possible. In SB/SE Collection Operations and Operations Support, the HOD is the assigned area DSA.

Note: If the SAA employee completes Form 11377 or Form 11377-E the primary manager **or**sharing manager may sign the form and forward to designated Head of Office Designee(HOD) by close of business or as soon as possible.

(4) Copies of Form 11377 or Forms 11377-E containing taxpayer data are not retained by the employee, the manager, or in any location other than with the IDRS Data Security Staff.

(5) The DSA uploads the Form 11377 or Form 11377-E, along with any attachments to the IRM 5.1.25.1.7 (2) within five business days of receipt. Files are retained for six years from the date they are uploaded. The naming convention is SEID-MMDDYYYY-##.

- SEID is the accessing employee
- MMDDYYYY is the date of the access, even if the form is completed later. For example, January 1, 2020 is 01012020.
- ## is the number of forms submitted on the same day for the same accessing employee; i.e. use 01 if it is the first submission and, 02 if it is the second submission, etc.

(6) The DSA responds promptly to requests from Labor Relations or TIGTA and provide copies of any Form 11377 or Form 11377-E needed for an ongoing UNAX investigation.

This Page Intentionally Left Blank

Exhibit 5.1.25-1 (10-16-2023)
Acronyms

The following is a list of acronyms used throughout this IRM.

Acronym	Definition
AIS	Automated Insolvency System
AMS	Accounts Management Services
AOIC	Automated Offers In Compromise
BEARS	Business Entitlement Access Request System
CASS	Collection Automation Support & Security
CFOL	Corporate Files On-Line
DSA	Data Security Analyst
DUL	Designated User Listing
ECC-MEM	Enterprise Computing Center - Memphis
ECC-MTB	Enterprise Computing Center - Martinsburg
EOPS	Enterprise Operations
HOD	Head of Office Designee
IAT	Integrated Automation Technologies
ICS	Integrated Collection System
IDRS	Integrated Data Retrieval System
IORS	IDRS Online Reports Services
IT	Information Technology
IUUD	IDRS Unit and USR Database
Mef-RRD	Modernized e-File Return Request and Display
MPAF	Maximum Profile Authorization File
PAR	Personnel Action Request
SAA	Shared Administrative Associate
SAAS	Security Audit and Analysis System
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TDS	Transcript Delivery System
TIN	Taxpayer Identification Number
TSA	Terminal Security Administrator
TSID	Terminal Security Identification

Exhibit 5.1.25-1 (Cont. 1) (10-16-2023)
Acronyms

Acronym	Definition
UCCP	Unit Command Code Profile
UNAX	Unauthorized Access
USR	Unit Security Representative

Exhibit 5.1.25-2 (10-16-2023)
Common Command Codes - SB/SE Collection Operations and Operations Support

Exhibit 5.1.25-2 (Cont. 1) (10-16-2023)
Common Command Codes - SB/SE Collection Operations and Operations Support

Exhibit 5.1.25-2 (Cont. 2) (10-16-2023)
Common Command Codes - SB/SE Collection Operations and Operations Support

Exhibit 5.1.25-2 (Cont. 3) (10-16-2023)
Common Command Codes - SB/SE Collection Operations and Operations Support

#
#
#
#
#