



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.34

APRIL 10, 2025

EFFECTIVE DATE

(04-10-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.34, *Information Technology (IT) Security, IDRS Security Controls*.

MATERIAL CHANGES

- (1) 10.8.34.1, Program Scope and Objectives - Updated subsection to align with standard security policy language.
- (2) 10.8.34.1.1, Background - Updated subsection to align with standard security policy language.
- (3) 10.8.34.1.2, Authority - Updated subsection to align with standard security policy language.
- (4) 10.8.34.1.3, Roles and Responsibilities - Updated subsection to align with standard security policy language.
- (5) 10.8.34.1.4, Program Management and Review - Updated subsection to align with standard security policy language.
- (6) 10.8.34.1.5, Program Controls - Updated subsection to align with standard security policy language.
- (7) 10.8.34.1.6, Terms and Acronyms - Updated subsection to align with standard security policy language.
- (8) 10.8.34.1.7, Related Resources - Updated subsection to align with standard security policy language.
- (9) 10.8.34.2, Risk Acceptance and Risk-Based Decisions (RBD) - Renamed subsection and updated subsection to align with standard security policy language.
- (10) 10.8.34.3, Integrated Data Retrieval System (IDRS) - Relocated subsection to 10.8.34.4.
- (11) 10.8.34.4, IDRS Security System - Relocated subsection to 10.8.34.4.1.
- (12) 10.8.34.5, Authorized Access - Relocated subsection to 10.8.34.4.3. Removed “\” within (2) bullet.
- (13) 10.8.34.6, Communications Protocol - Relocated subsection to 10.8.34.4.4.
- (14) 10.8.34.7, IDRS Roles and Responsibilities - Relocated subsection to 10.8.34.3 to align with standard security policy language.
- (15) 10.8.34.7.1, IDRS, Key Governance and Related Roles & Responsibilities - Removed subsection.
- (16) 10.8.34.7.1.1, Senior Management/Executives - Relocated subsection to 10.8.34.3.1.
- (17) 10.8.34.7.1.2, IDRS Security Program Officer - Relocated subsection to 10.8.34.3.1.1.
- (18) 10.8.34.7.1.3, Manager - Relocated subsection to 10.8.34.3.2. Removed (5) which duplicates 10.8.34.1.3 (1).
- (19) 10.8.34.7.2, Organization/Functional Roles and Responsibilities - Removed subsection.

- (20) 10.8.34.7.2.1, IDRS Security Program Management Office (SPMO) - Renamed subsection and relocated subsection to 10.8.34.4.2. For (3)(d), added a reference to Exhibit 10.8.34-3.
- (21) 10.8.34.7.2.2, IDRS Security Business Division Point of Contact (POC) - Updated title and relocated subsection to 10.8.34.3.3.
- (22) 10.8.34.7.2.3, IRS Information Technology (IRS IT) Cybersecurity, Security Operations & Standards Division (Cyber-SOSD) Management - Renamed subsection and relocated subsection to 10.8.34.3.1.2.
- (23) 10.8.34.7.2.4, IRS Information Technology (IRS IT) Cybersecurity Operations Management - Relocated subsection to 10.8.34.3.1.3.
- (24) 10.8.34.7.2.5, IDRS Security Account Administrator - Relocated subsection to 10.8.34.3.4. Updated (5)(b) to add language relocated from 10.8.2.3.1.31 (6).
- (25) 10.8.34.7.2.6, Computing Center IDRS Security Administrator - Relocated subsection to 10.8.34.3.5. Qualified first use of “ACS” and “ICS”.
- (26) 10.8.34.7.2.7, IDRS Security Analyst - Relocated subsection to 10.8.34.3.6. Added a requirement from 10.8.2.3.1.30 (4). Added (2), which was relocated from 10.8.2.3.1.30 (4).
- (27) 10.8.34.7.2.7.1, Campus IDRS Security Analyst - Relocated subsection to 10.8.34.3.6.1.
- (28) 10.8.34.7.2.7.2, Computing Center IDRS Security Analyst - Relocated subsection to 10.8.34.3.6.2.
- (29) 10.8.34.7.2.8, Unit Security Representative (USR) - Relocated subsection to 10.8.34.3.7. Removed “\” within (11)(c) bullet.
- (30) 10.8.34.7.2.9, Alternate USR - Relocated subsection to 10.8.34.3.8.
- (31) 10.8.34.7.2.10, Terminal Security Administrator (TSA) - Relocated subsection to 10.8.34.3.9. Added a space within “13230shall”.
- (32) 10.8.34.7.2.11, IORS Report Reviewer - Relocated subsection to 10.8.34.3.10.
- (33) 10.8.34.7.2.11.1, IORS Primary Report Reviewer - Relocated subsection to 10.8.34.3.10.1.
- (34) 10.8.34.7.2.11.2, IORS Secondary Report Reviewer - Relocated subsection to 10.8.34.3.10.2.
- (35) 10.8.34.8, Management Controls - Relocated subsection to 10.8.34.5. Updated NIST control family name for “CA” and “PL”.
- (36) 10.8.34.8.1, Security Planning - Relocated subsection to 10.8.34.5.1.
- (37) 10.8.34.8.1.1, Rules of Behavior - Relocated subsection to 10.8.34.5.1.1.
- (38) 10.8.34.9, Operational Controls - Relocated subsection to 10.8.34.6. Updated NIST control family name for “AT”.
- (39) 10.8.34.9.1, Security Awareness and Training - Relocated subsection to 10.8.34.6.1.
- (40) 10.8.34.9.1.1, Awareness - Relocated subsection to 10.8.34.6.1.1.
- (41) 10.8.34.9.1.1.1, IDRS User Security Awareness Training - Relocated subsection to 10.8.34.6.1.1.1.
- (42) 10.8.34.9.1.2, Training - Relocated subsection to 10.8.34.6.1.2.
- (43) 10.8.34.9.1.2.1, Manager Training - Relocated subsection to 10.8.34.6.1.2.1.

-
- (44) 10.8.34.9.1.2.2, IDRS Security Program Management Office (SPMO) Staff Training - Renamed subsection and relocated subsection to 10.8.34.6.1.2.2.
 - (45) 10.8.34.9.1.2.3, IDRS Security Analyst and Computing Center IDRS Security Analyst Training - Relocated subsection to 10.8.34.6.1.2.3.
 - (46) 10.8.34.9.1.2.4, IDRS Security Account Administrator and Computing Center IDRS Security Administrator Training - Relocated subsection to 10.8.34.6.1.2.4.
 - (47) 10.8.34.9.1.2.5, Unit Security Representative (USR) and Alternate USR Training - Relocated subsection to 10.8.34.6.1.2.5.
 - (48) 10.8.34.9.1.2.5.1, Course Development and Revision - Relocated subsection to 10.8.34.6.1.2.5.1.
 - (49) 10.8.34.9.1.2.5.2, Initial Training - Relocated subsection to 10.8.34.6.1.2.5.2.
 - (50) 10.8.34.9.1.2.5.3, Annual Refresher Training - Relocated subsection to 10.8.34.6.1.2.5.3.
 - (51) 10.8.34.9.1.2.5.4, Unit Security Representative (USR) Training Annual Compliance Review - Renamed subsection and relocated subsection to 10.8.34.6.1.2.5.4.
 - (52) 10.8.34.9.1.2.6, Terminal Security Administrator (TSA) Training - Relocated subsection to 10.8.34.6.1.2.6.
 - (53) 10.8.34.9.2, Media Protection - Relocated subsection to 10.8.34.6.2.
 - (54) 10.8.34.10, Technical Controls - Relocated subsection to 10.8.34.7.
 - (55) 10.8.34.10.1, Identification and Authentication - Relocated subsection to 10.8.34.7.1.
 - (56) 10.8.34.10.1.1, User Identification and Authentication - Relocated subsection to 10.8.34.7.1.1. Qualified the first use of "PIN" and "PIV".
 - (57) 10.8.34.10.1.2, IDRS Employee Number - Relocated subsection to 10.8.34.7.1.2.
 - (58) 10.8.34.10.1.3, Workstation Identification and Authentication - Relocated subsection to 10.8.34.7.1.3.
 - (59) 10.8.34.10.1.3.1, IDRS Terminals - Relocated subsection to 10.8.34.7.1.3.1. Qualified first use of "TSID".
 - (60) 10.8.34.10.1.3.2, Designation of Terminals - Relocated subsection to 10.8.34.7.1.3.2. Qualified first use of "TRDB".
 - (61) 10.8.34.10.1.3.3, Location of Terminals - Relocated subsection to 10.8.34.7.1.3.3.
 - (62) 10.8.34.10.1.3.4, Terminal Vector Record (TVR) File - Renamed subsection and relocated subsection to 10.8.34.7.1.3.4.
 - (63) 10.8.34.10.1.3.5, Terminal Security Lock-Out - Relocated subsection to 10.8.34.7.1.3.5.
 - (64) 10.8.34.10.1.3.6, Terminal Shutdowns During Emergencies - Relocated subsection to 10.8.34.7.1.3.6.
 - (65) 10.8.34.10.1.4, Password Management - Relocated subsection to 10.8.34.7.1.4.
 - (66) 10.8.34.10.1.4.1, Temporary Passwords - Relocated subsection to 10.8.34.7.1.4.1.
 - (67) 10.8.34.10.1.4.2, User-Created Passwords - Relocated subsection to 10.8.34.7.1.4.2. Added a note to (1) about multi-factor authentication (MFA).

- (68) 10.8.34.10.1.4.3, Password Documentation - Relocated subsection to 10.8.34.7.1.4.3.
- (69) 10.8.34.10.1.4.4, IDRS Password Management Capability - Renamed subsection and relocated subsection to 10.8.34.7.1.4.4.
- (70) 10.8.34.10.2, Access Control - Relocated subsection to 10.8.34.7.2.
- (71) 10.8.34.10.2.1, Account Management - Relocated subsection to 10.8.34.7.2.1.
- (72) 10.8.34.10.2.1.1, Establishing IDRS Units - Relocated subsection to 10.8.34.7.2.1.1.
- (73) 10.8.34.10.2.1.2, Adding Employees to IDRS/Assigning Employee Numbers - Relocated subsection to 10.8.34.7.2.1.2. Corrected “entitlements” to “entitlement” within (1)(c). Updated title for IRM 10.23.3 within (4). Replaced AWSS with FMSS within (5).
- (74) 10.8.34.10.2.1.2.1, Adding National Headquarters Personnel to IDRS - Relocated subsection to 10.8.34.7.2.1.2.1. Removed language about “block 23” within (3). Block 23 language original referred to OL5081, which BEARS has replaced.
- (75) 10.8.34.10.2.1.2.2, Adding IRS Information Technology (IT) Staff to IDRS - Relocated subsection to 10.8.34.7.2.1.2.2.
- (76) 10.8.34.10.2.1.2.3, Adding Personnel from Treasury Inspector General Tax Administration - Relocated subsection to 10.8.34.7.2.1.2.3.
- (77) 10.8.34.10.2.1.2.4, Adding IRS Information Technology (IRS IT) Cyber-SOSD Personnel - Renamed subsection and relocated subsection to 10.8.34.7.2.1.2.4.
- (78) 10.8.34.10.2.1.2.5, Adding IRS Information Technology (IRS IT) Cybersecurity Personnel - Relocated subsection to 10.8.34.7.2.1.2.5.
- (79) 10.8.34.10.2.1.2.6, Adding Contractor Personnel - Relocated subsection to 10.8.34.7.2.1.2.6.
- (80) 10.8.34.10.2.1.3, Protection of the IDRS User - Relocated subsection to 10.8.34.7.2.1.3.
- (81) 10.8.34.10.2.1.4, Transferring Employees between IDRS Units/Changing Employee Numbers - Relocated subsection to 10.8.34.7.2.1.4.
- (82) 10.8.34.10.2.1.5, Authorizing IDRS User Access to Other IRS Campuses’ Databases (Multiple Accesses Capability) - Relocated subsection to 10.8.34.7.2.1.5.
- (83) 10.8.34.10.2.1.6, Unit and User Profiles - Relocated subsection to 10.8.34.7.2.1.6.
- (84) 10.8.34.10.2.1.6.1 Maximum Profile Authorization File (MPAF) - Renamed and relocated subsection to 10.8.34.7.2.1.6.1.
- (85) 10.8.34.10.2.1.6.2, Unit Command Code Profile (UCCP) - Relocated subsection to 10.8.34.7.2.1.6.2. Added a closing period within the Note for (7).
- (86) 10.8.34.10.2.1.6.3, Limited Profile - Relocated subsection to 10.8.34.7.2.1.6.3.
- (87) 10.8.34.10.2.1.6.4, Employee Security Record File (ESRF) - Relocated subsection to 10.8.34.7.2.1.6.4.
- (88) 10.8.34.10.2.1.6.5, Establishing and Updating the Unit MPAF and UCCP - Relocated subsection to 10.8.34.7.2.1.6.5.
- (89) 10.8.34.10.2.1.6.6, Sensitive Command Codes and Sensitive Command Code Combinations - Relocated subsection to 10.8.34.7.2.1.6.6.

-
- (90) 10.8.34.10.2.1.6.7, Command Codes with Sensitive Connotation - Renamed to Command Codes with Sensitive Connotations. Relocated subsection to 10.8.34.7.2.1.6.7.
 - (91) 10.8.34.10.2.1.6.8, Automated Command Code Access Control - Relocated subsection to 10.8.34.7.2.1.6.8.
 - (92) 10.8.34.10.2.1.7, IDRS Organization Code Management - Relocated subsection to 10.8.34.7.2.1.7. Added a note about Exhibit 10.8.34.20 to (1).
 - (93) 10.8.34.10.2.1.8, IDRS Security Documentation - Relocated subsection to 10.8.34.7.2.1.8.
 - (94) 10.8.34.10.2.1.8.1, BEARS Entitlements - Relocated subsection to 10.8.34.7.2.1.8.1.
 - (95) 10.8.34.10.2.1.8.2, Form 9937 IDRS Unit Request - Relocated subsection to 10.8.34.7.2.1.8.2.
 - (96) 10.8.34.10.2.1.8.3, Form 13230 IDRS Security Personnel Designation - Relocated subsection to 10.8.34.7.2.1.8.3.
 - (97) 10.8.34.10.2.1.8.4, Completion of Security Documentation - Relocated subsection to 10.8.34.7.2.1.8.4.
 - (98) 10.8.34.10.2.1.9, IDRS Unit and USR Database (IUUD) - Renamed and relocated subsection to 10.8.34.7.2.1.9.
 - (99) 10.8.34.10.2.1.10, IDRS Security Command Codes - Renamed and relocated subsection to 10.8.34.7.2.1.10. Updated "add and delete units" to "add/delete units" for consistency.
 - (100) 10.8.34.10.2.1.10.1, IDRS Security Command Codes for IDRS Users - Relocated subsection to 10.8.34.7.2.1.10.1.
 - (101) 10.8.34.10.2.1.10.2, Command Codes Restricted to IDRS Security Account Administrators - Relocated subsection to 10.8.34.7.2.1.10.2.
 - (102) 10.8.34.10.2.1.10.3, Command Codes Restricted to IDRS Users - Relocated subsection to 10.8.34.7.2.1.10.3.
 - (103) 10.8.34.10.2.1.10.4, Command Codes Restricted to IDRS Security Program Office - Relocated subsection to 10.8.34.7.2.1.10.4.
 - (104) 10.8.34.10.2.1.10.5, Command Codes Restricted to Computing Center IDRS Security Administrators - Relocated subsection to 10.8.34.7.2.1.10.5.
 - (105) 10.8.34.10.2.1.10.6, Command Codes Restricted to Campus Submission Processing Accounting Department Staff - Relocated subsection to 10.8.34.7.2.1.10.6.
 - (106) 10.8.34.10.2.1.10.7, Command Codes Authorized for Use by Unit Security Representatives (USRs) - Renamed and relocated subsection to 10.8.34.7.2.1.10.7. Corrected command code "BYPASS" to "BYPAS" within (2).
 - (107) 10.8.34.10.2.1.10.8, Command Codes Authorized for Use by IDRS Terminal Security Administrators (TSAs) - Renamed and relocated subsection to 10.8.34.7.2.1.10.8.
 - (108) 10.8.34.10.2.2, Access Enforcement - Relocated subsection to 10.8.34.7.2.2.
 - (109) 10.8.34.10.2.2.1, Security Violations - Relocated subsection to 10.8.34.7.2.2.1.
 - (110) 10.8.34.10.2.2.2, Security Violation Errors - Relocated subsection to 10.8.34.7.2.2.2.
 - (111) 10.8.34.10.2.2.3, IDRS Workstations/Terminals - Relocated subsection to 10.8.34.7.2.2.3.

- (112) 10.8.34.10.2.2.3.1, Signing Off from IDRS - Renamed subsection and relocated subsection to 10.8.34.7.2.2.3.1.
- (113) 10.8.34.10.2.2.3.2, Locking of IDRS Workstations/Terminals - Relocated subsection to 10.8.34.7.2.2.3.2.
- (114) 10.8.34.10.2.2.3.3, Unlocking Workstations/Terminals - Relocated subsection to 10.8.34.7.2.2.3.3.
- (115) 10.8.34.10.2.2.3.4, Session Lockout and Termination (Automatic Session Lockout) - Relocated subsection to 10.8.34.7.2.2.3.4. Applied IG Memo IT-10-0224-0002, *IDRS Security Controls Automatic Session Lockout*.
- (116) 10.8.34.10.2.2.4, IDRS User Accounts - Relocated subsection to 10.8.34.7.2.2.4.
- (117) 10.8.34.10.2.2.4.1, Locking of IDRS User Accounts - Relocated subsection to 10.8.34.7.2.2.4.1.
- (118) 10.8.34.10.2.2.4.2, Employee Self-Profile Locking (LOKME) - Relocated subsection to 10.8.34.7.2.2.4.2.
- (119) 10.8.34.10.2.2.4.3, Automatic Account Lockout Due to Inactivity - Relocated subsection to 10.8.34.7.2.2.4.3.
- (120) 10.8.34.10.2.2.4.4, Unlocking IDRS User Accounts - Relocated subsection to 10.8.34.7.2.2.4.4.
- (121) 10.8.34.10.2.2.4.5, Deleting Employee Access to IDRS - Relocated subsection to 10.8.34.7.2.2.4.5.
- (122) 10.8.34.10.2.2.4.6, Automatic Account Deletion Due to Inactivity - Relocated subsection to 10.8.34.7.2.2.4.6.
- (123) 10.8.34.10.2.2.4.7, IDRS Automated Delete and Lock Enhancement Due to Personnel Action - Relocated subsection to 10.8.34.7.2.2.4.7.
- (124) 10.8.34.10.2.2.4.8, Command Code Deletions - Relocated subsection to 10.8.34.7.2.2.4.8.
- (125) 10.8.34.10.2.2.5, Locking of IDRS Units - Relocated subsection to 10.8.34.7.2.2.5.
- (126) 10.8.34.10.2.3, Unsuccessful Login Attempts - Relocated subsection to 10.8.34.7.2.3.
- (127) 10.8.34.10.2.4, Concurrent Session Control - Relocated subsection to 10.8.34.7.2.4.
- (128) 10.8.34.10.2.4.1, Dual SINON to IDRS - Relocated subsection to 10.8.34.7.2.4.1. Added a note about Exhibit 10.8.34-21 and Exhibit 10.8.34-22 to (5).
- (129) 10.8.34.10.2.5, Least Privilege - Relocated subsection to 10.8.34.7.2.5.
- (130) 10.8.34.10.3, Audit and Accountability - Relocated subsection to 10.8.34.7.3.
- (131) 10.8.34.10.3.1, IDRS Security Reports - Relocated subsection to 10.8.34.7.3.1.
- (132) 10.8.34.10.3.1.1, IDRS Online Reports Services (IORS) - Relocated subsection to 10.8.34.7.3.1.1. Updated “web based” to “web-based” within (2). Updated “concern” to “concerns” within (10)(e).
- (133) 10.8.34.10.3.1.2, Review and Certification of Security Reports in IORS - Relocated subsection to 10.8.34.7.3.1.2.
- (134) 10.8.34.10.3.1.2.1, Security Reports Requiring Certification by an IDRS Security Account Administrator - Relocated subsection to 10.8.34.7.3.1.2.1.

- (135) 10.8.34.10.3.1.2.2, Security Reports Requiring Certification by an IDRS Security Analyst - Relocated subsection to 10.8.34.7.3.1.2.2.
- (136) 10.8.34.10.3.1.2.3, Security Reports Requiring Certification by a Primary Report Reviewer - Relocated subsection to 10.8.34.7.3.1.2.3.
- (137) 10.8.34.10.3.2, Audit Trails - Relocated subsection to 10.8.34.7.3.2. Added a comma after “assessed” within (2).
- (138) 10.8.34.10.3.2.1, Audit Trail Extracts - Relocated subsection to 10.8.34.7.3.2.1.
- (139) 10.8.34.10.3.2.1.1, UNAX Related and Suspected Criminal Activity Audit Trail Extract Requests - Relocated subsection to 10.8.34.7.3.2.1.1.
- (140) 10.8.34.10.3.2.1.2, Non-UNAX/Non-Criminally Related Activity Audit Trail Extract Requests - Relocated subsection to 10.8.34.7.3.2.1.2.
- (141) 10.8.34.10.3.2.1.3, Freedom of Information Act (FOIA) Audit Trail Extract Requests - Renamed and relocated subsection to 10.8.34.7.3.2.1.3.
- (142) 10.8.34.10.3.2.1.4, Electronic Discovery Requests - Relocated subsection to 10.8.34.7.3.2.1.4.
- (143) 10.8.34.10.3.2.2, Requesting Audit Trail Extracts - Relocated subsection to 10.8.34.7.3.2.2.
- (144) 10.8.34.10.3.2.2.1, Processing of Audit Trail Extracts by the Cybersecurity Computing Center Operations Staff (IAD IDRS Audit Trail Extracts) - Relocated subsection to 10.8.34.7.3.2.2.1. Updated “KISAM” to “help desk” in (1). Updated “was” to “were” within (4).
- (145) 10.8.34.10.3.2.2.2, Processing Audit Trail Extracts using the SAAS Application (SAAS IDRS Audit Trail Extracts) - Relocated subsection to 10.8.34.7.3.2.2.2.
- (146) Exhibit 10.8.34-1, Glossary - Removed subsection to align with standard security policy language. Content was relocated to Exhibit 10.8.34-2, Terms and Acronyms.
- (147) Exhibit 10.8.34-2, Terms and Acronyms - Relocated exhibit to Exhibit 10.8.34-1. Removed sentence preceding the table. Updated column titles within the table, Added acronyms ACS, BMF, CCNIP, CISA, CMMI, EFC, ELC, EO, GMF, ICS, ITIL, LSS, NARA, PIN, PIV, SP, SPMO, SRM, and TS. Added terms IDRS Security Account Administrator and IDRS Security Analyst. Removed terms Campus IDRS Security Officer, entity index, entity module, and dummy module. Qualified the first use of “FISMA”, “IMF”, “ISRP”, and “PII”. Updated title for Treasury Departmental Incident Response Plan (IRP) for term “breach”. Corrected qualification of FISMA. Corrected qualification of CCNIP to “Case Creation Non-Filter Identification Process”.
- (148) Exhibit 10.8.34-3, Related Resources - Relocated exhibit to Exhibit 10.8.34-2. Table of resources was converted to a list of resources. IRMs 2.3 series, 2.4 series, 2.9.1, 10.9.1, and 10.23.3 were added. Documents 12926-SA, 12926-USR, and 12990 were added. Forms 9936, 9937, 9937-A, 11370-A, 13230, and 14665 were added. Publication Treasury Departmental Incident Response Plan (IRP) was added. The revision version and date for NIST Special Publication 800-53 was updated.
- (149) Exhibit 10.8.34-4, Distribution Procedures - Relocated exhibit to Exhibit 10.8.34-3.
- (150) Exhibit 10.8.34-5, Command Codes Marked as Sensitive in the IDRS Command Code Table - Relocated exhibit to Exhibit 10.8.34-4.
- (151) Exhibit 10.8.34-6, Sensitive Command Code Combinations - Relocated exhibit to Exhibit 10.8.34-5.
- (152) Exhibit 10.8.34-7, Command Codes with Sensitive Connotations - Relocated exhibit to Exhibit 10.8.34-6.

- (153) Exhibit 10.8.34-8, Restricted Command Codes for the Role: Revenue Agents, Tax Compliance Officers/Tax Specialists, Estate Tax Attorneys, and (SBSE) Headquarters Analysts who do not require command code ESTAB (RSTRK Definer A) - Relocated exhibit to Exhibit 10.8.34-7.
- (154) Exhibit 10.8.34-9, Restricted Command Codes for the Role: “Manual Refund Authorizers and Manual Refund Certifying Officers” (RSTRK Definer M) - Relocated exhibit to Exhibit 10.8.34-8.
- (155) Exhibit 10.8.34-10, Restricted Command Codes for Roles: SB/SE Headquarters Analysts (who require command code ESTAB), 809 Receipt Book Users, and Submission Processing employees that issue, verify, or reconcile Blank Form 809 (RSTRK Definer R) - Relocated exhibit to Exhibit 10.8.34-9.
- (156) Exhibit 10.8.34-11, Restricted Command Codes for the Role: Remittance Perfection Technicians Who Do Not Have Blank Form 809 Responsibilities (RSTRK Definer U) - Relocated exhibit to Exhibit 10.8.34-10.
- (157) Exhibit 10.8.34-12, IDRS Office Identifiers (OIs), Organization Code Ranges, and Unpostable Holding Units - Renamed exhibit and relocated exhibit to Exhibit 10.8.34-11.
- (158) Exhibit 10.8.34-13, IDRS Organization Codes – IRS Campuses - Relocated exhibit to Exhibit 10.8.34-12.
- (159) Exhibit 10.8.34-14, IDRS Organization Codes – Taxpayer Services (TS) Area Offices - Renamed exhibit and relocated exhibit to Exhibit 10.8.34-13.
- (160) Exhibit 10.8.34-15, IDRS Organization Codes – Small Business/Self-Employed (SB/SE) Area Offices - Renamed exhibit and relocated exhibit to Exhibit 10.8.34-14.
- (161) Exhibit 10.8.34-16, IDRS Organization Codes - Other Business Divisions - Relocated exhibit to Exhibit 10.8.34-15. Updated “Large and Midsize Business” to “Large Business and International”.
- (162) Exhibit 10.8.34-17, IDRS Audit Trail Record Format – Security Audit and Analysis System (SAAS) - Relocated exhibit to Exhibit 10.8.34-16. Removed duplicated language. Added paragraph restriction for sentence with website information.
- (163) Exhibit 10.8.34-18, IDRS Audit Trail Record Format – ICS/ACS/Print (IAP) - Relocated exhibit to Exhibit 10.8.34-17.
- (164) Exhibit 10.8.34-19, Campus TSID Domain Index Table - Relocated exhibit to Exhibit 10.8.34-18. Corrected “Following” to “The following”.
- (165) Exhibit 10.8.34-20, Automated Delete and Lock System Rules - Relocated exhibit to Exhibit 10.8.34-19.
- (166) Exhibit 10.8.34-21, IDRS Applications and Command Codes with IDRS Organization Code Controls - Relocated exhibit to Exhibit 10.8.34-20. Updated “Nation-wide” to “Nationwide”. Marked unpostable holding unit for “Ogden” as “NA”.
- (167) Exhibit 10.8.34-22, Generalized Unpostable Framework (GUF) Unpostable Table Conversions for Campus Functions - Relocated exhibit to Exhibit 10.8.34-21.
- (168) Exhibit 10.8.34-23, Generalized Unpostable Framework (GUF) Unpostable Table Conversions for Area Office and Other Business Organization Functions - Relocated exhibit to Exhibit 10.8.34-22.
- (169) Throughout the IRM, updated Wage & Investment (W&I) to Taxpayer Services (TS).
- (170) Throughout the IRM, updated Enterprise Operations, Security Operations & Standards Division (EOPS-SOSD) to Cybersecurity, Security Operations & Standards Division (Cyber-SOSD).

- (171) Throughout the IRM, updated “HR Connect” to “HRConnect”.
- (172) Throughout the IRM, updated “shall” to “must”.
- (173) Throughout the IRM, removed capitalization, as appropriate, i.e., within names of roles and responsibilities.
- (174) Throughout the IRM, replaced “e-mail” with “email”.
- (175) Throughout the IRM, updated to a consistent structure when referencing “BEARS “<action>” entitlement request”.
- (176) Throughout the IRM, added and italicized titles, as appropriate.
- (177) Throughout the IRM, updated “section” to “subsection”, as appropriate.
- (178) Throughout the IRM, hyphenated “security related”.
- (179) Throughout the IRM, replaced “thru” with “through”.
- (180) Throughout the IRM, corrected use of terminology “log on”, “log off”, “sign on”, and “sign off”, as appropriate.
- (181) Throughout the IRM, replaced “web site” with “website”.
- (182) Throughout the IRM, removed all instances of “naked links” to internal sites, that only IRS employees can access, per Office of Online Services (OLD), Privacy, Governmental Liaison and Disclosure (PGLD) and Information Technology (IT).
- (183) Throughout the IRM, created additional hyperlinks.
- (184) Throughout the IRM, updated use of numbers to spell out and only spell out “0”-“9” and ordinal values for “0”-“9”.
- (185) Throughout the IRM, replaced language with acronyms, when appropriate.
 - a. “BI” for “background investigation”
 - b. “EAD” for “Effective Action Difference”
 - c. “SOSD” for “Security Operations & Standards Division”
 - d. “IDRS” for “Integrated Data Retrieval System”
 - e. “IORS” for “IDRS Online Reports Services”
 - f. “IUUD” for “IDRS Unit and USR Database”
 - g. “MPAF” for “Maximum Profile Authorization File”
 - h. “OI” for “office identifier”
 - i. “POC” for “point of contact”
 - j. “SPMO” for “Security Program Management Office”
 - k. “SSN” for “Social Security number”
 - l. “TIGTA” for “Treasury Inspector General for Tax Administration”
 - m. “TSA” for “Terminal Security Administrator”
 - n. “UCCP” for “Unit Command Code Profile”
 - o. “UNAX” for “unauthorized access”
 - p. “USR” for “Unit Security Representative”
- (186) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM. Reviewed and updated plain language, grammar, titles, website addresses, legal references, and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes all prior versions of IRM 10.8.34. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, and IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*. This IRM incorporates IG Memo IT-10-0224-0002, *IDRS Security Controls Automatic Session Lockout*, dated April 17, 2024.

AUDIENCE

All personnel responsible for ensuring Integrated Data Retrieval System (IDRS) security. This IRM applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

10.8.34

IDRS Security Controls

Table of Contents

10.8.34.1 Program Scope and Objectives

10.8.34.1.1 Background

10.8.34.1.2 Authority

10.8.34.1.3 Roles and Responsibilities

10.8.34.1.4 Program Management and Review

10.8.34.1.5 Program Controls

10.8.34.1.6 Terms and Acronyms

10.8.34.1.7 Related Resources

10.8.34.2 Risk Acceptance and Risk-Based Decisions (RBD)

10.8.34.3 IDRS Roles and Responsibilities

10.8.34.3.1 Senior Management/Executives

10.8.34.3.1.1 IDRS Security Program Officer

10.8.34.3.1.2 IRS Information Technology (IRS IT) Cybersecurity, Security Operations & Standards
Division (Cyber-SOSD) Management

10.8.34.3.1.3 IRS Information Technology (IRS IT) Cybersecurity Operations Management

10.8.34.3.2 Manager

10.8.34.3.3 IDRS Security Business Division Point of Contact (POC)

10.8.34.3.4 IDRS Security Account Administrator

10.8.34.3.5 Computing Center IDRS Security Administrator

10.8.34.3.6 IDRS Security Analyst

10.8.34.3.6.1 Campus IDRS Security Analyst

#

10.8.34.3.7 Unit Security Representative (USR)

10.8.34.3.8 Alternate USR

10.8.34.3.9 Terminal Security Administrator (TSA)

10.8.34.3.10 IORS Report Reviewer

10.8.34.3.10.1 IORS Primary Report Reviewer

10.8.34.3.10.2 IORS Secondary Report Reviewer

10.8.34.4 Integrated Data Retrieval System (IDRS)

10.8.34.4.1 IDRS Security System

10.8.34.4.2 IDRS Security Program Management Office (SPMO)

10.8.34.4.3 Authorized Access

10.8.34.4.4 Communications Protocol

10.8.34.5 Management Controls

10.8.34.5.1 Security Planning

10.8.34.5.1.1	Rules of Behavior	
10.8.34.6	Operational Controls	
10.8.34.6.1	Security Awareness and Training	
10.8.34.6.1.1	Awareness	
10.8.34.6.1.1.1	IDRS User Security Awareness Training	
10.8.34.6.1.2	Training	
10.8.34.6.1.2.1	Manager Training	
10.8.34.6.1.2.2	IDRS Security Program Management Office (SPMO) Staff Training	
10.8.34.6.1.2.3	IDRS Security Analyst and Computing Center IDRS Security Analyst Training	
10.8.34.6.1.2.4	IDRS Security Account Administrator and Computing Center IDRS Security Administrator Training	
10.8.34.6.1.2.5	Unit Security Representative (USR) and Alternate USR Training	
10.8.34.6.1.2.5.1	Course Development and Revision	
10.8.34.6.1.2.5.2	Initial Training	
10.8.34.6.1.2.5.3	Annual Refresher Training	
10.8.34.6.1.2.5.4	Unit Security Representative (USR) Training Annual Compliance Review	
10.8.34.6.1.2.6	Terminal Security Administrator (TSA) Training	#
10.8.34.7	Technical Controls	
10.8.34.7.1	Identification and Authentication	
10.8.34.7.1.1	User Identification and Authentication	
		#
10.8.34.7.1.3	Workstation Identification and Authentication	
		#
10.8.34.7.1.3.2	Designation of Terminals	
10.8.34.7.1.3.3	Location of Terminals	
		#
		#
10.8.34.7.1.3.6	Terminal Shutdowns During Emergencies	
		#
		#
		#
		#
		#
10.8.34.7.2	Access Control	
		#
		#
		#
		#

[illegible]

#####

#

0.8.34.7.3.1.1 IDRS Online Reports Services (IORS)

10.8.34.7.3.1.2.1 Security Reports Requiring Certification by an IDRS Security Account Administrator

10.8.34.7.3.1.2.2 Security Reports Requiring Certification by an IDRS Security Analyst

10.8.34.7.3.1.2.3 Security Reports Requiring Certification by a Primary Report Reviewer

10.8.34.7.3.2.1.1 UNAX Related and Suspected Criminal Activity Audit Trail Extract Requests

10.8.34.7.3.2.1.2 Non-UNAX/Non-Criminally Related Activity Audit Trail Extract Requests

10.8.34.7.3.2.1.3 Freedom of Information Act Audit Trail Extract Requests

10.8.34.7.3.2.1.4 Electronic Discovery Requests

10.8.34.7.3.2.2 Requesting Audit Trail Extracts

10.8.34.7.3.2.2.1 Processing of Audit Trail Extracts by the Cybersecurity Computing Center Operations Staff (IAP IDRS Audit Trail Extracts)

10.8.34.7.3.2.2.2 Processing Audit Trail Extracts using the SAAS Application (SAAS IDRS Audit Trail Extracts)

Exhibits

10.8.34-1 Terms and Acronyms

10.8.34-2 Related Resources

10.8.34-3 Distribution Procedures

#

10.8.34-11 IDRS Office Identifiers, Organization Code Ranges, and Unpostable Holding Units

10.8.34-12 IDRS Organization Codes — IRS Campuses

10.8.34-13 IDRS Organization Codes - Taxpayer Services (TS) Area Offices

10.8.34-14 IDRS Organization Codes - Small Business/Self-Employed (SB/SE) Area Offices

10.8.34-15 IDRS Organization Codes - Other Business Divisions

10.8.34-16 IDRS Audit Trail Record Format — Security Audit and Analysis System (SAAS)

10.8.34-17 IDRS Audit Trail Record Format — ICS/ACS/Print (IAP)

#

10.8.34.1
(04-10-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of the Integrated Data Retrieval System (IDRS) within the IRS.
 - a. This IRM is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS IDRS for on-premises systems, including on-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this IRM apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate information systems that store, process, or transmit IRS information or connect to an IRS network or system.
 - c. All NIST impact-level baselines (i.e., Low, Moderate, High), unless a requirement indicates differently.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cyber security, Cybersecurity Threat Response and Remediation
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.34.1.1
(04-10-2025)
Background

- (1) The term IDRS, in the context of this policy, is inclusive of Corporate Files On-Line (CFOL) and the Security and Communications System (SACS).
- (2) IRM 10.8.34 is part of the IRM Part 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.34.1.2
(04-10-2025)
Authority

- (1) All IRS systems and applications are required to comply with executive orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.

10.8.34.1.3
(04-10-2025)
Roles and Responsibilities

- (1) The IRS must implement security roles in accordance with federal laws and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions. The roles and responsibilities are defined in IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.
- (2) Supplemental roles and responsibilities specific to the implementation of IDRS security controls (if any) are located in IRM 10.8.34.3, IDRS Roles and Responsibilities.

10.8.34.1.4
(04-10-2025)
**Program Management
and Review**

- (1) The IRS security policy program establishes a framework of controls to ensure the inclusion of security into the IRS IT environment. This framework is provided through the issuance of security policies via the IRM 10.8 series and the development of security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.
- (2) It is the policy of the IRS to:
 - a. Establish and manage an information security program within all its organizations. This IRM provides uniform policies and guidance to be used by each organization.
 - b. Protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access (UNAX) to that IT resource.
 - c. Protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.34.1.5
(04-10-2025)
Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirements checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the revision process.
- (3) For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance on protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets.
- (5) In the event there is a discrepancy between this IRM and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this IRM are more restrictive.

10.8.34.1.6
(04-10-2025)
Terms and Acronyms

- (1) Refer to Exhibit 10.8.34-1, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.34.1.7
(04-10-2025)
Related Resources

- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.34-2, Related Resources, for a list of related resources and references.

10.8.34.2
(04-10-2025)
Risk Acceptance and Risk-Based Decisions (RBD)

- (1) Any exception to this IRM requires the authorizing official (AO) to make a risk acceptance decision.
- (2) Users must submit risk-based decision (RBD) requests in accordance with Cybersecurity's Security Risk Management (SRM) risk acceptance process documented in the Request for Risk Acceptance and Risk Based Decision (RBD) Standard Operating Procedures (SOP).

Note: Users can access RBD documentation in the FISMA Doc Library on the Enterprise FISMA (EFC)

RBD Documentation site.

- (3) Refer to IRM 10.8.1 for additional guidance on risk acceptance and RBDs.

10.8.34.3
(04-10-2025)
IDRS Roles and Responsibilities

- (1) The following supplemental roles and responsibilities are specific to the implementation of IDRS security controls.

10.8.34.3.1
(04-10-2025)
Senior Management/ Executives

- (1) Senior management/executives are officials subordinate to the Commissioner.
- (2) Senior management/executives have responsibility for the implementation and administration of IDRS security.
- (3) Senior management/executives must perform the following IDRS responsibilities:
 - a. Ensure IDRS Security policies and guidance are implemented.
 - b. Identify at least one individual as the point of contact (POC) and coordinator for IDRS security activities. The security role of these individuals is IDRS security business division POC. The POCs name, standard employee identifier (SEID), and contact information must be provided to the IDRS Security Program Management Office (SPMO).
 - c. Ensure unit security representatives (USRs) and IDRS Online Reports Services (IORS) primary report reviewers are appointed to cover all IDRS units and users.
 - d. Ensure for each IDRS unit, IDRS security account administrators are provided with the name, SEID, and contact information for all current USRs, alternate USRs, Terminal Security Administrators (TSAs), and IORS security report reviewers.
 - e. Ensure the IDRS security account administrators or the IDRS SPMO are notified of any business division reorganizations that may require the realignment or renumbering of IDRS units.
 - f. Ensure IDRS security issues are the topic of discussion at managerial meetings annually at a minimum.
 - g. Ensure IDRS security reports are reviewed, and certified timely; and that any required report actions are completed timely.
 - h. Ensure corrective actions are taken when IDRS security report reviewers fail to meet IDRS security report responsibilities.

10.8 Information Technology (IT) Security

- i. Ensure that the required responses related to IDRS security report compliance are submitted timely to the IDRS SPMO and/or Cybersecurity Operations staff.
- j. Ensure that all reported accesses and violations for USRs and alternate USRs are independently reviewed at the next management level that is higher than the URS's or alternate URS's level.
- k. Ensure any user who is being investigated for a UNAX violation is promptly removed from IDRS.
- l. Ensure all users who have a proven UNAX violation have satisfied all requirements of disciplinary actions before being added to IDRS.
- m. Ensure USRs and alternate USRs complete the required initial and annual refresher training.
- n. Ensure IDRS users complete the required initial and annual refresher awareness training.
- o. Ensure IDRS users recertify (re-acknowledge) the rules of behavior annually to maintain access privileges.
- p. Fulfill any additional IDRS security responsibilities of the senior management/executive stated elsewhere in this IRM.

10.8.34.3.1.1
(04-10-2025)
**IDRS Security Program
Officer**

- (1) The IDRS security program officer is the senior manager/executive (or designee) responsible for ensuring that the appropriate IDRS security posture is maintained.
- (2) The Director, Cybersecurity Architecture & Implementation (or designee) serves as the IDRS security program officer.

10.8.34.3.1.2
(04-10-2025)
**IRS Information
Technology (IRS IT)
Cybersecurity, Security
Operations & Standards
Division (Cyber-SOSD)
Management**

- (1) IRS IT Cybersecurity, Security Operations & Standards Division (Cyber-SOSD) management must assign security specialist(s) and/or security assistants as IDRS security account administrators.
- (2) IRS IT Cyber-SOSD management must assign security specialist(s) and/or security assistants as computing center IDRS security administrators.

#

10.8.34.3.1.3
(04-10-2025)
**IRS Information
Technology (IRS IT)
Cybersecurity
Operations Management**

- (1) IRS IT Cybersecurity Operations management assigns security specialist(s) and/or security assistants as campus IDRS security analysts.

- (2) IRS IT Cybersecurity Operations management assigns security specialist(s) and/or security assistants as computing center IDRS security analysts.

#

10.8.34.3.2
(04-10-2025)
Manager

- (1) The manager of IDRS users must be responsible for day-to-day implementation and administration of IDRS security.
- (2) The manager must perform the following IDRS responsibilities:
- a. Ensure IDRS Security policies and guidance are implemented.
 - b. Reinforce employee awareness and compliance with UNAX rules prohibiting access to any taxpayer or personnel data not required to accomplish official duties.
 - c. Conduct periodic re-orientation sessions to ensure employees remain alert and aware of IDRS security requirements.
 - d. Ensure employees who are IDRS users complete the required initial and annual refresher training.
 - e. Ensure weekly and monthly IDRS Security reports are reviewed and certified timely and that any required report actions are completed timely.
 - f. Ensure the Maximum Profile Authorization File (MPAF), the Unit Command Code Profile (UCCP), and the Employee Security Record File (ESRF) for all employees and IDRS units are reviewed at least monthly, and any necessary corrective actions are completed timely.
 - g. Ensure the command code usage of employees with sensitive command code combinations is reviewed at least monthly.
 - h. Ensure new IDRS users review the rules of behavior and that each IDRS user recertifies the rules of behavior annually via the Business Entitlement Access Request System (BEARS).
 - i. Ensure questionable activity or potential UNAX violations are timely reported to the Treasury Inspector General for Tax Administration (TIGTA).
 - j. Report any IDRS user who refuses to certify or recertify the rules of behavior to the employee's division management for appropriate disciplinary action. Users who refuse to certify or recertify the rules of behavior will not be allowed to access IDRS and the user's IDRS user account must be deleted.
 - k. Ensure all requirements associated with a disciplinary action have been met prior to reinstating an IDRS user who has been deleted from IDRS because of an illegal or improper activity. If the employee's disciplinary action resulted because of one or more unauthorized actions, the manager must ensure the employee has met the recertification requirements, which includes having the employee review the UNAX briefing and signing Form

10.8 Information Technology (IT) Security

11370-A, *Recertification of UNAX Awareness Briefing*, before the employee may be added or re-added to IDRS or receives access to taxpayer information and return information. The manager's signature on the UNAX Recertification form indicates that the employee has met all disciplinary actions for recertification.

- I. Fulfill any additional IDRS security responsibilities of the manager stated elsewhere in this IRM.
- (3) Managers who have been officially designated as the USR for the unit/group (via an approved Form 13230, *IDRS Security Personnel Designation*) must perform the IDRS security duties of a USR as described by this IRM as well as the manager duties.
 - (4) Managers who have not been designated as the USR for the unit/group perform the following:
 - a. Coordinate with the USR to help ensure IDRS security is effectively implemented for the unit/group.
 - b. Ensure the USR is notified immediately, when an IDRS user no longer needs system access.
 - c. Provide the USR with written or electronic documentation for all requests to update the unit's MPAF or UCCP or to update an employee's ESRF.
- 10.8.34.3.3
(04-10-2025)
**IDRS Security Business
Division Point of
Contact (POC)**
- (1) The IDRS security business division POC helps ensure the POC's business organization effectively performs IDRS security administration and monitoring.
 - (2) IRS business divisions are required to identify at least one individual as the IDRS security business division POC.
 - (3) The IDRS security business division POC must:
 - a. Serve as the business organization's POC with the IDRS SPMO.
 - b. Serve as a liaison between the IDRS SPMO and the business organization in addressing IDRS security issues.
 - c. Coordinate the business organization's response to IDRS security-related issues.
 - d. Coordinate the business organization's response to IORS security report certification related issues.
 - e. Represent the business organization at IDRS security-related stakeholder meetings.
 - f. Fulfill any additional IDRS security responsibilities of the IDRS security business division POC stated elsewhere in this IRM.

#

- (5) IDRS security business division POCs who are bargaining unit employees:

#

##

#

(6) Additional duties may be assigned by respective business divisions due to the differing needs of each business area.

- (1) The IDRS security account administrator performs tasks relating to the administration of IDRS user and unit accounts.
- (2) The IDRS security account administrator must be a non-bargaining unit employee who is a member of the Cyber-SOSD staff.
- (3) To help ensure proper separation of duties, the IDRS security account administrator must not simultaneously serve as the computing center IDRS security administrator.

#[illegible]

[illegible]

10.8.34.3.5
(04-10-2025)

**Computing Center IDRS
Security Administrator**

- (1) The computing center IDRS security administrator performs tasks relating to the administration of computing center IDRS security activity.
- (2) The computing center IDRS security administrator must be a non-bargaining unit employee who is a member of the Cyber-SOSD staff.
- (3) To help ensure proper separation of duties, the computing center IDRS security administrator must not simultaneously serve as IDRS security account administrator.

#

10.8.34.3.6
(04-10-2025)

IDRS Security Analyst

- (1) The IDRS security analyst performs IDRS security policy support and oversight related tasks for IDRS campus domains and/or IDRS computing centers.
- (2) The IDRS security analyst must be a non-bargaining unit employee who is a member of the Cybersecurity Operations staff.

10.8.34.3.6.1
(04-10-2025)

**Campus IDRS Security
Analyst**

- (1) The campus IDRS security analyst performs IDRS security policy support and oversight related tasks for the IDRS campus domains.
- (2) The campus IDRS security analyst must be a non-bargaining unit employee who is a member of the Cybersecurity Operations staff.

#

[illegible]

#

#

#

#

#

[illegible]

[illegible]

##

- (1) The alternate USR is an individual who assists and/or performs the duties of the primary USR when that individual is not available.
- (2) Alternate USR designations must be approved by a second level or higher manager who is in the direct chain of command of the IDRS users being supported.
 - a. The designation must be submitted to an IDRS security account administrator on Form 13230.
 - b. Before submission, the Form 13230 must be coordinated with the primary USR(s) to ensure the primary USR(s) is aware of who is being designated as an alternate USR.
- (3) The alternate USR must be a non-bargaining unit employee or a bargaining unit employee (e.g., lead) who is familiar with IDRS security requirements and procedures.
- (4) The alternate USR must have a “completed” BI status.
- (5) The alternate USR must complete:

- a. Initial USR training prior to performing USR duties.
 - b. USR refresher training at least annually.
- (6) The alternate USR's manager must submit a BEARS, "Modify User Profile" request to the IDRS security account administration staff to request the appropriate security command codes be included in the alternate USR's IDRS employee profile. The BEARS entitlement request must be approved by the alternate USR's primary USR to ensure the primary USR is aware of who is being given security command codes.
 - (7) A non-bargaining unit alternate USR is authorized to act as the primary USR when the primary USR is not available, including serving as a unit's primary report reviewer for the review and certification of security reports. A non-bargaining unit alternate USR may perform all related security duties when officially acting as the primary USR and is authorized to have the full suite of USR security command codes.
 - (8) A bargaining unit alternate USR cannot act as primary USR and cannot perform the full duties of a USR. They support a non-bargaining unit USR and can perform nonmanagerial duties of the USR, such as updating a user's profile. The bargaining unit alternate USR must not review another employee's IDRS actions.
 - (9) For IDRS security purposes, the alternate USR's security activity is under the purview of the designated primary USR for that unit or area. If the primary USR has concerns regarding security actions taken by the alternate USR, the primary USR may request that the IDRS security analyst provide an audit trail extract of the alternate USR's activities for a designated date or date range.
 - (10) The alternate USR must fulfill any additional IDRS security responsibilities of the alternate USR stated elsewhere in this IRM.

10.8.34.3.9
(04-10-2025)

**Terminal Security
Administrator (TSA)**

- (1) The TSA is an individual assigned by a business organization to unlock IDRS terminals and unlock employee profiles locked due to 17 days of inactivity.
- (2) Assigning individuals to serve as a TSA is optional and the discretion of management for the business organization. The intent of the TSA role is to reduce USR workload.
- (3) TSAs may either be a non-bargaining or bargaining unit employee.
- (4) A TSA designation must be approved by a second level manager or higher in the TSA's business organization. The designation must be submitted to the IDRS Security Account Administration staff on Form 13230. Before submission, the Form 13230 must be coordinated with the unit's primary USR to ensure the primary USR is aware of who is being designated as a TSA.
- (5) The TSA's manager must submit a BEARS "modify user" entitlement request to the IDRS security account administrator to have the appropriate security command codes added to the TSA's IDRS employee profile. The BEARS entitlement request application must be approved by the TSA's primary USR to ensure the primary USR is aware of who is being given security command codes.
- (6) TSAs will not be required to complete specialized IDRS security training but must receive instruction from a primary USR before performing TSA duties.

- (7) Command Code SECOP is to be placed in the user profile of TSAs (SECOP is the command code used to unlock IDRS terminals). At the request of the manager, TSAs may also be given command code UNLEM. (UNLEM is the command code used by a TSA to unlock an employee profile that has been locked by the system because the user has been inactive for 17 days).
- (8) For TSAs who are given the capability to unlock employee profiles, USRs are authorized to provide a copy of the "Master Register of Active Users" report or a Command Code SFINQA screen print to the TSA that lists the IDRS employee numbers of users in the TSA's unit(s). TSAs are only authorized to unlock IDRS profiles for known users.
- (9) For IDRS security purposes, the TSA's security activity is under the purview of the designated primary USR(s) for that unit or area. If the primary USR has concerns regarding security actions taken by the TSA, the primary USR may request that an IDRS security analyst provide an audit trail extract of the TSA activities for a designated date or date range.

10.8.34.3.10
(04-10-2025)
IODS Report Reviewer

- (1) The IORS report reviewer is an individual assigned by the reviewer's business organization to review IDRS security reports in IORS.
- (2) There are two IORS report reviewer roles:
 - a. IORS primary report reviewer
 - b. IORS secondary report reviewer

10.8.34.3.10.1
(04-10-2025)
IODS Primary Report Reviewer

- (1) The IORS primary report reviewer is an individual assigned by the reviewer's business organization who is responsible for ensuring that the IDRS security reports for a designated IDRS unit(s) are timely reviewed and the appropriate actions are taken when necessary.
- (2) IORS primary report reviewers must be non-bargaining unit employees. They normally serve as the unit's manager, USR, or have an IDRS coordinator's role.
- (3) Each IDRS unit must have a designated IORS primary report reviewer, who must be submitted to the IDRS security account administration staff on Form 13230. Before submission, Form 13230 must be coordinated with the primary USR(s) to ensure the primary USR(s) is aware of who is being designated as the IORS primary report reviewer.
- (4) The IDRS security account administration staff must lock any unit that has active IDRS users, but where no IORS primary report reviewer has been designated to review/certify IDRS security reports. The IDRS security account administrator must also designate the primary USR for the unit as the IORS primary report reviewer until the IDRS security account administration staff is notified to the contrary.
- (5) The IORS primary report reviewer roles are recorded in the IUUD. This information is used by IORS to define primary report reviewer permissions in IORS.
- (6) The primary report reviewer must input report certifications but may indicate in the certification that the certification is based on the documented review of others such as the manager or USR, if the primary report reviewer does not perform either of these roles.

- (7) The IORS primary report reviewer will receive notification when the security reports are available for review and when security reports requiring certification have not been certified within the prescribed time frame.
- (8) The primary report reviewer may grant a proxy to another non-bargaining unit IORS user to act in the reviewer's place when the reviewer is not available.
- (9) The IORS primary report reviewer may grant secondary report reviewer permissions to other IORS users to view and comment on IDRS security reports for the unit. The IORS primary report reviewer must remove these permissions when they are no longer needed.
- (10) The IORS primary report reviewer must fulfill any additional IDRS security responsibilities of the IORS primary report reviewer stated elsewhere in this IRM.

10.8.34.3.10.2

(04-10-2025)

ORS Secondary Report Reviewer

- (1) The IORS secondary report reviewer is an individual who has received permissions from an IORS primary report reviewer to view one or more security reports for a unit.
- (2) The IORS secondary report reviewer is usually the manager of a unit where the primary report reviewer role is being performed by another individual.
- (3) The IORS secondary report reviewer must be a non-bargaining unit employee. However, bargaining unit employees (e.g., leads) who are experienced with IDRS may be given secondary reviewer permissions to assist the primary report reviewer with the review and evaluation of security reports that do not involve the review of another employee's IDRS actions. These are reports that do not require a certification (the Master Register, Employee Count, Automated IDRS Sign-offs, and Password Management Activations reports). Bargaining unit employees must not review reports that involve another employee's IDRS actions. These reports include the Security Violations, Sensitive Access, and Monthly and Quarterly Security Profile reports.
- (4) The IORS secondary report reviewer cannot input certifications for security responsibilities of the IORS secondary report reviewer stated elsewhere in this IRM.

10.8.34.4

(04-10-2025)

Integrated Data Retrieval System (IDRS)

- (1) IDRS is designed primarily to accomplish the following:
 - a. Provide employees with instantaneous access to the taxpayer.
 - b. Provide better, faster, more responsive, and more personal service to the taxpayer.
 - c. Facilitate and speed the work of employees in campuses and area offices by providing the most current information on tax accounts and by furnishing the most up-to-date data processing tools available today.
- (2) IDRS capabilities include abilities to:
 - a. Research taxpayer account information.
 - b. Request tax returns and account transcripts.
 - c. Input transactions, such as adjustments, entity changes, etc.
 - d. Input collection information for storage and processing in the system.
 - e. Generate notices, collection documents, and other outputs.

- (3) Each user account is associated with an IDRS unit that is associated with a campus IDRS database.
- (4) Each campus database is associated with one of two computing centers listed below:
 - a. Enterprise Computing Center - Martinsburg (ECC-MTB):
 - Campus databases that are associated with ECC-MTB are: Andover, Austin, Brookhaven, Ogden, and Philadelphia.
 - b. Enterprise Computing Center - Memphis (ECC-MEM):
 - Campus databases that are associated with ECC-MEM are: Atlanta, Cincinnati, Fresno, Kansas City, and Memphis.

10.8.34.4.1
(04-10-2025)
IDRS Security System

- (1) The Security and Communications System (SACS) is the IDRS security system that provides security and auditing for IDRS.
 - The SACS is designed to meet IRS-defined security controls and the security controls defined in IRM 10.8.1.
- (2) SACS provides identification and authorization for every input:
 - a. The system's employee security file contains significant data required to recognize each employee authorized to use IDRS.
 - b. The system's terminal security file includes terminal identification to recognize each workstation capable of accessing IDRS.
- (3) All actions taken on IDRS, both authorized and unauthorized, are recorded in the IDRS audit trail.
- (4) The IDRS security system is designed to provide protection to both the taxpayer and IDRS user.
 - The taxpayer must be protected from UNAX, inspection, changes, and disclosure of any of the taxpayer's personal information and tax related information.
 - The IDRS user employee must be protected from other personnel using personnel identification to access or make changes to an account.

10.8.34.4.2
(04-10-2025)
**IDRS Security Program
Management Office
(SPMO)**

- (1) The IDRS SPMO is a function in the IRS Information Technology (IRS IT), Cybersecurity organization that was established to manage the IDRS security program.
- (2) The IDRS SPMO consists of the following:
 - a. IDRS security program officer - the senior manager/executive (or designee) responsible for ensuring that the appropriate IDRS security posture is maintained.
 - b. IDRS security program manager - the individual who coordinates day-to-day IDRS SPMO activity.
 - c. IDRS security program analyst(s) - individuals who support the day-to-day IDRS SPMO activity.
- (3) The IDRS SPMO must perform the following:
 - a. Establish policy and procedures for managing the IRS IDRS Security Program.

- b. Identify security activities that will help improve IDRS security.
- c. Perform activities that promote and maintain a continuing awareness of IDRS security.
- d. Disseminate information to IRS management, IDRS Security personnel, and IDRS users regarding changes in policy, procedures, and practices. Refer to Exhibit 10.8.34-3, Distribution Procedures, for additional details.
- e. Provide IDRS Security subject matter expert support to IRS management and staff.
- f. Define the minimum content required for IDRS user security awareness training.
- g. Develop, review, and update the required initial and annual refresher training for USRs; and monitor compliance with the training requirement.
- h. Review the implementation of IDRS security at IRS campuses, computing centers, field offices, and other locations.
- i. Evaluate the implementation of IDRS security by IDRS security account administrators, IDRS security analysts, USRs, and business unit management. Any oversight and evaluation activities performed by or for the IDRS SPMO must not substitute or replace any monitoring, training, or oversight activities required to be performed by IDRS security account administrators, IDRS security analysts, USRs, or business unit management.
- j. Support Cybersecurity staff in the review of requests to deviate from IDRS security policy stated in this IRM.
- k. Fulfill any additional IDRS security responsibilities of the IDRS SPMO stated elsewhere in this IRM.

10.8.34.4.3
(04-10-2025)

Authorized Access

- (1) IDRS users must only access accounts necessary for accomplishing official duties.
- (2) IDRS user must not access:
 - The user's spouse and any ex-spouses
 - The user's children
 - The user's parents and grandparents
 - Anyone living in the user's household
 - The user's other close relatives
 - Friends or neighbors with whom the user has close relationships
 - Celebrities, when the information is not needed to carry out tax related duties
 - An individual or organization for which the user or the user's spouse is an officer, trustee, general partner, agent, attorney, consultant, contractor, employee, or member
 - Any other individual or organization with which the user may have a personal or outside business relationship that could raise questions about the user's lack of impartiality in handling the tax matter
 - Any other individual unless access is required by the user's duties as assigned by management
- (3) IDRS users must not access the account of any taxpayer or another IRS employee unless there is a business need and access has been formally authorized as part of the user's official duties.
- (4) The willful unauthorized access or inspection of taxpayer records is referred to as UNAX.

- a. Refer to IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*.
- (5) Under the Taxpayer Browsing Protection Act (Public Law No. 105-35):
- a. Willful unauthorized disclosure, access or inspection of non-computerized taxpayer records, including hard copies of returns - as well as computerized information - is a crime, punishable upon conviction, by fines, prison terms and termination of employment.
 - b. Taxpayers have the right to take legal action when taxpayers are victims of unlawful access or inspection - even if a taxpayer's information is never revealed to a third party.
 - c. When managers or employees are criminally charged, the Service is required to notify taxpayers that taxpayers' records have been accessed without authorization.
- (6) The provisions and applicable criminal penalties under the Taxpayer Browsing Protection Act also apply to all vendors, contractors, and contractor employees.

10.8.34.4.4
(04-10-2025)
**Communications
Protocol**

- (1) This subsection defines the communications protocol to be followed when addressing IDRS security issues.
- (2) Unless otherwise stated, the IDRS user must direct IDRS security-related concerns to the user's manager or USR.
- (3) Unless otherwise stated, managers and USRs must elevate the following:
- a. Any IDRS account administration-related concern the managers and USRs are unable to resolve to the IDRS Security Account Administration staff.
 - b. Any IDRS security report-related concern the managers and USRs are unable to resolve to the manager's and USR's home campus Cybersecurity IDRS security analyst.
 - c. Any IDRS security policy-related concern the managers and USRs are unable to resolve to the IDRS SPMO.
- (4) Unless otherwise stated, the IDRS security account administration staff and Cybersecurity IDRS security analysts must elevate any IDRS security-related concern the staff and analysts are unable to resolve to the IDRS SPMO.
- (5) IDRS security business division POCs must direct IDRS security related concerns to the IDRS SPMO or the Cybersecurity IDRS security analysts that support the POC's business organization.
- (6) IDRS security-related concerns that involve multiple business divisions or campus domains must be elevated to the IDRS SPMO.
- (7) IDRS users, managers, or USRs rarely have a need to contact a computing center's IDRS security staff. Unless otherwise stated, any communication with computing center IDRS security staff must be routed through the IDRS SPMO.

10.8.34.5
(04-10-2025)

Management Controls

- (1) Per IRM 10.8.1, IRS must implement management security controls to mitigate risk of IT applications and electronic information loss to protect the organization's mission. In addition to the management security control guidance defined within this IRM, requirements for the following management security control areas must be implemented in accordance with IRM 10.8.1:

- CA - Assessment, Authorization, and Monitoring
- PL - Planning
- RA - Risk Assessment
- SA - System and Service Acquisition
- SR - Supply Chain Risk Management

10.8.34.5.1
(04-10-2025)

Security Planning

- (1) Per IRM 10.8.1, the IRS must establish enterprise-wide security planning policy and procedures that define and implement rules of behavior for all IT systems.

10.8.34.5.1.1
(04-10-2025)

Rules of Behavior

- (1) IDRS users must sign a statement acknowledging that they have read and understand the rules of behavior.
- (2) The BEARS system must be used to document IDRS users' acknowledgement they have read and understand the rules of behavior.
- a. Prior to being added to IDRS, users must sign the BEARS rules of behavior statement acknowledging that they have read and understand the rules.
 - b. To maintain access privileges, IDRS users must annually sign the BEARS rules of behavior statement to recertify (re-acknowledge) they have read and understand the rules of behavior.
- (3) IDRS users who do not sign or annually re-acknowledge the security rules will be denied access to the system. The manager of an employee who refuses to sign security rules, may at the discretion of business organization management, brief the employee on the security rules in the presence of a second manager and both managers acknowledge in writing that the employee was briefed on the security rules.
- (4) Failure to comply with the rules of behavior is subject to disciplinary actions. Refer to IRM 6.751.1, *Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance*, for further guidance.

10.8.34.6
(04-10-2025)

Operational Controls

- (1) Per IRM 10.8.1, IRS must implement operational security controls. In addition to the operational security control guidance defined within this IRM, requirements for the following operational security control areas must be implemented in accordance with IRM 10.8.1:

- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PE - Physical and Environmental Protection
- PS - Personnel Security
- PT - Personally Identifiable Information Processing and Transparency
- SI - System and Information Integrity

- 10.8.34.6.1.2.2
(04-10-2025)
IDRS Security Program Management Office (SPMO) Staff Training
- (1) The IDRS security program officer must ensure IDRS SPMO staff are properly trained to perform IDRS security-related tasks.
- 10.8.34.6.1.2.3
(04-10-2025)
IDRS Security Analyst and Computing Center IDRS Security Analyst Training
- (1) IRS IT Cybersecurity Operations management must ensure IDRS security analysts and computing center IDRS security analysts are properly trained to perform IDRS security-related tasks.
- 10.8.34.6.1.2.4
(04-10-2025)
IDRS Security Account Administrator and Computing Center IDRS Security Administrator Training
- (1) IRS IT Cyber-SOSD management must ensure IDRS security account administrators and computing center IDRS security administrators are properly trained to perform IDRS security-related tasks.
- 10.8.34.6.1.2.5
(04-10-2025)
Unit Security Representative (USR) and Alternate USR Training
- (1) Employees designated as USR or alternate USR must complete the required initial and annual refresher training.
- #

#
- 10.8.34.6.1.2.5.1
(04-10-2025)
Course Development and Revision
- (1) The IDRS SPMO must be responsible for developing and revising the required USR initial and annual refresher training.
- a. The IDRS SPMO must develop the required USR initial and annual refresher training courses and ensure the courses are available on the ITM system.
- b. The IDRS SPMO must review the required USR initial and annual refresher training courses at least annually by end of each calendar year to ensure they reflect current IDRS security policies and procedures.
- c. The IDRS SPMO must contact the IRS IT Learning & Education staff each year to notify staff if any course revisions are necessary.
- d. The IDRS SPMO must update the required USR initial and annual refresher training courses as necessary.
- 10.8.34.6.1.2.5.2
(04-10-2025)
Initial Training
- (1) Employees designated as USR or alternate USR must complete the ITM — IDRS USR Training.
- a. Security command codes must not be placed in the profiles any USR or alternate USR who has not completed this ITM course.
- b. Security command codes must be removed from the profile of any USR or alternate USR who has not completed this ITM course.

- c. Completing the course will satisfy the annual training requirement for the FISMA training year in which the course is completed.

Note: The FISMA training year is July 1 through June 30.

- (2) New USRs and alternate USRs must complete the required initial training course before security command codes are added to the USR's profile.
- (3) Returning USRs and alternate USRs who have not performed USR duties for more than one year must be considered new and are required to complete the initial training course before security command codes are added to the USR's profile.
- (4) IDRS security account administration staff must remove security command codes from the profile of any USR or alternate USR who received the command codes without completing the required initial training.

10.8.34.6.1.2.5.3
(04-10-2025)
**Annual Refresher
Training**

- (1) Employees designated as a USR or alternate USR must complete the ITM — IDRS USR Refresher Training.
- (2) USRs and alternate USRs must complete the required refresher training annually before the end of each FISMA training year.

Note: The FISMA training year ends June 30th of each year.

- (3) Security command codes must be removed from the profile of any USR or alternate USR who has not completed the required annual refresher training.
- (4) USRs and alternate USRs who have completed the required initial training course during a FISMA training year are not required to complete the annual refresher training that year. However, it is recommended that they do so.
- (5) USRs and alternate USRs must not complete annual refresher training in lieu of the required initial training. The ITM system has been configured to prevent users from taking the annual refresher training course before they have completed the initial training course.
- (6) The IDRS SPMO must send an email message to USRs and alternate USRs each year when the annual refresher training course is available on the ITM system.
 - a. The message must inform USRs and alternate USRs the training is available.
 - b. The message must inform USRs and alternate USRs of the date by which the training is to be completed.
 - c. The message must advise USRs and alternate USRs that the training is mandatory.
 - d. The message must be sent to every employee who has been designated as a current USR or alternate USR in the IUUD.
 - e. The message must be sent to the USR/alternate USR's official email address that appears in the Discovery Directory database.

10.8.34.6.1.2.5.4
(04-10-2025)

**Unit Security
Representative (USR)
Training Annual
Compliance Review**

- (1) The IDRS SPMO must conduct an annual review to monitor compliance with and enforce the IRM requirement that all USRs and alternate USRs complete the required initial and annual refresher training.
- (2) Thirty calendar days before the end of the FISMA training year, the IDRS SPMO must perform a compliance check to identify USRs and alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS SPMO must obtain an ITM listing of USRs and alternate USRs who have completed the required training.
 - b. The IDRS SPMO must use the ITM listing to identify USRs and alternate USRs who have not completed the required training.
 - c. The IDRS SPMO must send an email message to USRs and alternate USRs who have not completed the required training to remind USRs of the requirement to complete training and to remind USRs of the date by which the training is to be completed.
- (3) Fifteen calendar days before the end of the FISMA training year, the IDRS SPMO must perform a compliance check to identify USRs and alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS SPMO must obtain an ITM listing of USRs and alternate USRs who have completed the required training.
 - b. The IDRS SPMO must use the ITM listing to identify USRs and alternate USRs who have not completed the required training.
 - c. The IDRS SPMO must send an email message to USRs and alternate USRs who have not completed the required training to remind USRs of the requirement to complete training by the end of the FISMA training year. The email message must also remind the USR or alternate USR that security command codes will be removed from the profiles of those who fail to complete the required training.
- (4) No more than fifteen calendar days after the end of the FISMA training year, the IDRS SPMO must perform a compliance check to identify USRs and alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS SPMO must obtain an ITM listing of USRs and alternate USRs who have completed the training as required.
 - b. The IDRS SPMO must use the ITM listing to identify USRs and alternate USRs who have not completed the training as required.
 - c. The IDRS SPMO must send an email message to USRs and alternate USRs who have not completed the training as required (and the USR's manager of record) to inform the USR that the USR has not met the USR training requirement. The email message must advise the USR that the USR's name will be referred to the IDRS security account administration staff, for the removal of security command codes from the USR's profile, if the USR has not completed the required training in 15 calendar days.
 - d. The IDRS SPMO must send a list of USRs and alternate USRs who have not completed the training as required to the appropriate IDRS security business division POC.
- (5) No more than 30 workdays after the end of the FISMA training year, the IDRS SPMO must perform an annual compliance review to identify USRs and alternate USRs who have not completed the required initial and annual refresher training.

- a. The IDRS SPMO must obtain an ITM listing of USRs and alternate USRs who have completed the training as required.
 - b. The IDRS SPMO must use the ITM listing to identify USRs and alternate USRs who have not completed the training as required.
 - c. The IDRS SPMO must send an email message to USRs and alternate USRs who have not completed the training as required (and the USR's manager of record) to inform the USR that the USR has not met the USR training requirement and that the USR's name is being referred to the IDRS security account administration staff, for the removal of security command codes from the USR's profile.
- (6) No more than seven calendar days after completing its annual compliance review, the IDRS SPMO must send a list of USRs and alternate USRs who have not completed the training as required to the IDRS security account administration staff for the removal of security command codes from the profiles of the non-compliant USRs and alternate USRs.
- a. The IDRS security account administration staff must remove all security command codes (except REPTS) from the profiles of non-compliant USRs and alternate USRs within 30 calendar days after receipt of the listing.
 - b. The IDRS security account administration staff may initiate follow-up contact with USRs, alternate USRs, and/or the USR's business organization before removing security command codes from the profiles of non-compliant USRs and alternate USRs.
 - c. The IDRS security account administration staff must lock any unit that has active IDRS users but does not have at least one USR (primary or alternate) with the security command codes needed to support the unit.
 - d. The IDRS security account administration staff must notify USRs and alternate USRs (and the USR's manager of record) after security command codes have been removed from the USR's profile.
 - e. The IDRS security account administration staff must send the IDRS SPMO a list of the USRs and alternate USRs whose security command codes were removed.
 - f. The IDRS security account administration staff must not add security command codes to the profile of a non-compliant USR or alternate USR until they have completed the required training.
 - g. After the non-compliant USR completes the necessary training, the non-compliant USR must submit a training completion certificate and a BEARS entitlement request to the IDRS security account administration staff and request security command codes to be added back to the USR's profile. A new Form 13230 designation is not required.
- (7) The IDRS SPMO may conduct additional compliance checks and/or send additional reminder messages to help increase compliance with USR training requirements.

10.8.34.6.1.2.6
(04-10-2025)
**Terminal Security
Administrator (TSA)
Training**

- (1) The USR must ensure the TSA has been trained on the following before performing TSA duties:
- a. When and how to unlock IDRS terminals.
 - b. When and how to unlock user profiles (if the TSA has been authorized to do so).
 - c. To report any unusual circumstances to the USR.

10.8.34.6.2
(04-10-2025)

#

10.8.34.7
(04-10-2025)
Technical Controls

- (1) Per IRM 10.8.1, the IRS must implement technical security controls. In addition to the technical security control guidance defined within this IRM, requirements for the following technical security control areas must be implemented in accordance with IRM 10.8.1.
- AC - Access Control
 - AU - Audit and Accountability
 - IA - Identification and Authentication
 - SC - System and Communications Protection

10.8.34.7.1
(04-10-2025)
Identification and Authentication

- (1) Per IRM 10.8.1, the IRS must establish, implement, and document a policy and procedure for identifying, authenticating the identity of, and tracking the actions of individuals requiring access to the IRS IT systems. This IRM subsection further defines the identification and authentication requirements as they pertain to IDRS security.

10.8.34.7.1.1
(04-10-2025)
User Identification and Authentication

- (1) All users must have individual IDRS accounts to access IDRS and to perform work. Users must not share IDRS accounts.

#

10.8.34.7.1.2
(04-10-2025)

#

#

#

10.8.34.7.1.3
(04-10-2025)
Workstation
Identification and
Authentication

#

10.8.34.7.1.3.1
(04-10-2025)

#

#

#

#

#

#

10.8.34.7.1.3.2 (1) When advised by IRS IT Desktop Support that a terminal identification needs
(04-10-2025) to be added, changed, or deleted, the IDRS security account administrator
Designation of Terminals must make the change.

#

- (1) Generally, IDRS terminals must be located in areas that have controlled access. However, those terminals located in areas accessible to the public or non-IRS personnel must be located so that the display screen cannot be viewed by walk-in taxpayers or unauthorized personnel. Screens, partitions, file cabinets, etc., may be used for this purpose.

[illegible]

Note: Emergency closings may also include drills and exercises.

#

#

#

##

(1) Per IRM 10.8.1, the IRS must implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. Access control must follow the principle of least privilege and separation of duties. This IRM further defines the access control requirements found in IRM 10.8.1 as they pertain to IDRS security.

#

#####

##

#

#

#

#

#

#####

#

#

[illegible]

#

##

#

[illegible]

#

##

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

##

#####

#

[illegible]

#

#

[illegible]

#

##

#####

#####

##

##

##

#

##

#

#

#

#

[illegible]

[illegible]

[illegible]

#

#

##

#

10.8.34.7.3
(04-10-2025)
Audit and Accountability

- (1) Per IRM 10.8.1, the IRS must create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. This IRM subsection defines audit and accountability requirements as they pertain to IDRS security.

10.8.34.7.3.1
(04-10-2025)
IDRS Security Reports

- (1) SACS journals all transactions performed by IDRS users and most system transactions. Selected journal transactions are used to produce batch security reports which are available via the IORS Application. There are currently approximately 40 different IDRS security reports which are generated either daily, weekly, bi-weekly, monthly, or quarterly.
- (2) IDRS security reports must be reviewed to help detect unauthorized user activity or problems with IDRS. If an IDRS security personnel, USR, manager, or other report reviewer encounters any indication of illegal or improper activity, the reviewer must refer the case and findings to the proper management or TIGTA officials.
- (3) IDRS Security personnel must ensure any IDRS user found not to be following proper security measures (based on examination of the security reports, audit trail, etc.) must be advised through the proper organizational channels of the deficiency and of the appropriate action to be taken.
- (4) Appropriate managerial review and follow-up of the various security reports is essential to ensuring the integrity of IDRS. Managers/USRs have the option of forwarding a copy of all security reports to upper management via IORS or secured email for oversight review.
- (5) The reviewer of an IDRS security report must be independent. Reviewers must not be the reviewer of the reviewer's own transactions.

10.8.34.7.3.1.1
(04-10-2025)
IDRS Online Reports Services (IORS)

- (1) The IORS application is the primary repository for IDRS Security reports.
- (2) IORS is web-based application that makes IDRS security reports available online to IDRS security staff, IRS business organization primary report reviewers, and other authorized reviewers (USRs, coordinators, and managers).
 - a. IORS users are authorized to view security reports based on the user's permissions.
 - b. Users are only able to view data for IDRS units, users, and business organizations that the user has been given permission to access.

#

- (4) IDRS security reports in IORS are available to IDRS Security staff, IDRS business organization POCs, IORS report reviewers, USRs, and unit managers for the timely review via the IORS application.

- (5) IORS provides users with the ability to analyze data in the security reports via the sorting of data and structured query capability. These functions are designed to identify items of interest that the security staff may need to further review and to respond to questions about IDRS users, such as identifying the number of IDRS users or determining who has or is using specific command codes.
- (6) IORS provides for the online submission and processing of certain IDRS security-related forms.
- (7) IDRS Security staff, primary report reviewers, USRs, and managers are encouraged to work within the IORS application to review user actions and activities.
 - a. Primary report reviewers, USRs and managers are not encouraged to print, save, or send security reports outside of the IORS applications unless unusual circumstances occur.
 - b. If security reports are saved, printed, or transmitted, the report data must be protected.
 - c. Report data that is saved electronically must be encrypted.
 - d. Report data that is printed must be stored in a secured location.
 - e. Report data transmitted via email must be transmitted using secured email.
- (8) IORS uses the information from the IUUD to identify users who have been designated as primary report reviewers for one or more IDRS units.
- (9) Business organizations must ensure all IDRS units have properly designated primary report reviewers. IDRS security account administrators must lock an IDRS unit that has not designated a primary report reviewer to review/certify IDRS security reports.
- (10) IORS users are expected to be non-bargaining unit employees.
 - a. However, report reviewers with large workloads may submit a request with a justification to IDRS security account administration staff to enable an experienced bargaining unit IDRS user with a security background to assist in the review of the security reports for the primary report reviewer.
 - b. If such a request is granted, the bargaining unit personnel may be given access to IORS to assist in the analyses of the reports. This option is only available when extreme workloads would prevent the timely review of security reports.
 - c. Bargaining unit personnel may assist with the review and evaluation of security reports that do not involve the review of another employee's IDRS actions. These are reports that do not require a certification (the Master Register, Employee Count, Automated IDRS Sign-offs, and Password Management Activations reports).
 - d. Bargaining unit employees must not review reports that involve another employee's IDRS actions. These are the reports that require a certification (Weekly Security Violations Report, Weekly Sensitive Access Report, Monthly Security Profile Report), as well as the Quarterly Security Profile Report.
 - e. Bargaining unit employees are not authorized to perform any follow-up action with IDRS users based on any concerns identified in the IDRS security reports.

- 10.8.34.7.3.1.2
(04-10-2025)
**Review and Certification
of Security Reports in
IORS**

- # #

#
- # #

#
- # #

- ##

##

10.8.34.7.3.1.2.1
(04-10-2025)

**Security Reports
Requiring Certification
by an IDRS Security
Account Administrator**

- (1) The following daily security reports must be timely reviewed and certified by the IDRS security account administrator:
 - Completed Command Code Inputs by IDRS Security Account Administrator and System
 - TAPS Error Report
 - Non-Processed Changing BOD
- (2) For the Completed Command Code Inputs by IDRS Security Account Administrator and System report, the IDRS security account administrator is required to:
 - a. Ensure appropriate and approved documentation is available to support all transactions for users who were added to IDRS, provided new temporary passwords, and given new capabilities to existing users.
 - b. Ensure security transactions were input properly with the correct information.
 - c. Perform random reviews of other transactions where inappropriate activity could compromise the use of IDRS.
- (3) For the TAPS Error Report, the IDRS security account administrator is required to:
 - a. Determine whether the individual listed in this report should have been deleted, locked or transferred to another IDRS unit. Once determined, either the USR or the IDRS security account administrator must take the appropriate action.
- (4) For the Non-Processed Changing BOD report, the IDRS security account administrator is required to:
 - a. Determine whether the individual listed in this report is in the correct IDRS unit. IDRS users who are not in the correct unit or who no longer need access to IDRS must be deleted immediately by either the IDRS security account administrator or USR.
- (5) Campus IDRS security account administrators are encouraged to review these reports as they become available but must certify these reports within seven calendar days for the certification to be considered timely.
- (6) IORS will provide a reminder notification on the fifth calendar day when a report has not been certified.
- (7) IDRS security account administrators are required, as of part of the certification, to identify the report level actions taken and to include any additional comments that will further explain any overall actions. Only users authorized to view report level information can see these entries.

10.8.34.7.3.1.2.2
(04-10-2025)

**Security Reports
Requiring Certification
by an IDRS Security
Analyst**

- (8) IORS also provides the ability for the IDRS security account administrator to enter detailed status and comments next to the specific transaction or activity. IDRS security account administrators are encouraged to use the detailed status and comments sections to provide additional information about the action taken. Only users authorized to view the report can see the entered information.
- (1) The following daily security reports must be timely reviewed and certified by the Cybersecurity IDRS security analyst:
 - a. Access to Own and Own Spouse by Accessing Employee.
- (2) For the Access to Own and Own Spouse by Accessing Employee report, the IDRS security analyst is required to:
 - a. Report all accesses to own or own spouse/former spouse tax accounts to TIGTA and all attempted accesses to the FMSS Labor Relations Office responsible for the accessing employee's business division. All accesses must be sent to the appropriate Labor Relations Office within five calendar days of the transaction occurrences.
 - b. Report all attempted or actual access to own or own spouse/ex-spouse tax accounts by TIGTA IDRS users to TIGTA Special Inquiries and Intelligence Division (SIID).
- (3) IDRS security analysts are encouraged to review this report as they become available but must certify the report within seven calendar days for the certification to be considered timely.
- (4) IORS will provide a reminder notification on the fifth calendar day when a report has not been certified.
- (5) IDRS security analysts are required, as of part of the certification, to identify the report level actions taken and to include any additional comments that will further explain any overall actions. Only users authorized to view report level information can see these entries.
- (6) IORS also provides the ability for the IDRS security analyst to enter detailed status and comments next to the specific transaction or activity. IDRS security analysts are encouraged to use the detailed status and comments sections to provide additional information about the action taken. Only users authorized to view the report can see the entered information.

10.8.34.7.3.1.2.3
(04-10-2025)

**Security Reports
Requiring Certification
by a Primary Report
Reviewer**

- (1) The primary report reviewer is required to review and certify the following security reports for the reviewer's IDRS unit(s):
 - Weekly Access to Employee and Employee Spouse by Accessing Employee
 - Weekly Security Violations Report
 - Monthly IDRS Security Profile Report
- (2) For the Weekly Access to Employee and Employee Spouse by Accessing Employee report, the primary report reviewer is required to:
 - a. Verify that all attempted or actual accesses to the account of other employees (or the spouse/former spouse of other employees) were performed for authorized business purposes.

- b. Confirm that users are adhering to the requirement of not accessing any account belonging to other employees (or the spouse/former spouse of other employees) who the user may know.
- c. Closely examine the appropriateness any accesses to accounts of other employees in the same business division, organization location, or geographical area.
- d. Use whatever tools are available to determine that the access was performed for business reasons, including, but not limited to, IDRS research, file source document reviews, and employee interviews.
- e. Report questionable accesses to TIGTA for follow-up.

[illegible]

#

- (5) Business organization primary report reviewers and designated secondary recipients are encouraged to review these reports as they become available, but the primary report reviewer must certify weekly reports within 14 calendar days and the monthly report within 28 days for the certifications to be considered timely.
- (6) IORS will provide a reminder notification to the primary report reviewer after 10 days for weekly reports and after 24 days for monthly reports if the report has not been certified.
- (7) Primary report reviewers are required, as part of the certification, to identify the report level actions taken and to include any additional comments that will further explain any overall actions. Cybersecurity and Cyber-SOSD IDRS security staff, the business organization POCs, and the primary report reviewer and the reviewer's manager authorized oversight viewing rights can see report level information.
- (8) IORS also provides the ability for the primary and secondary report reviewers to enter detailed status and comments next to the specific transaction or activity. Primary and secondary report reviewers are encouraged to use the detailed status and comments sections to provide additional information about the action taken. Only users authorized to view the report for the specific IDRS unit can see the entered detailed information.

10.8.34.7.3.2
(04-10-2025)#

#

#

#

#

#

#

- (1) Audit trail extracts are useful tools for managers and security staff to identify what transactions have been performed in the past.
- (2) Requests for extracts of audit trails for non-criminal activities, including employee integrity issues, security concerns, and requests for information under the Freedom of Information Act (FOIA), must be submitted to an IDRS security analyst for review and processing.
- (3) Refer to IRM 10.8.34.7.3.2.2, Requesting Audit Trail Extracts, for how to request an audit trail extract.

- (1) Managers must attempt to determine the appropriateness of any questionable accesses to taxpayer records by discussing the access with the employee who made the access and by reviewing transcripts, limited audit trail extracts, and other available documentation that could show the appropriateness of the access.
- (2) Management must refer cases to the local TIGTA office if the manager is not satisfied with the employee's response or if transcripts and other available documentation fail to demonstrate that the access is valid.
- (3) TIGTA must perform extracts of audit trails when the reasons for the requests are to support the review of potential UNAX or other criminal activities.
- (4) Managers who submit requests to the local TIGTA office are encouraged to keep a record of all referrals to TIGTA including the date and the source of the information that resulted in the referral.
- (5) Cybersecurity IDRS security analysts must immediately return audit trail extract requests to the authorizing manager with instructions to resubmit to the local TIGTA office if the manager:
 - a. Believes the individual may have committed a UNAX violation.

- b. Wants to determine whether the employee performed an unauthorized, inappropriate, or illegal action on IDRS, such as changing a taxpayer's address to redirect a refund.
- (6) The Cybersecurity IDRS security analyst may accept requests from managers who want to validate an employee's claim that the access to a taxpayer's account was the result of an error.
- (7) Managers are authorized to request audit extracts to support an employee's claim of an error or to enable a manager to confirm or refute an employee's explanation.
 - a. Any accesses that cannot be immediately determined to be appropriate by the manager must be forwarded to TIGTA for further review.
 - b. All other questionable accesses are to be referred to TIGTA for further review.
- (8) The Cybersecurity IDRS security analyst must contact the IDRS SPMO for determination on the appropriate routing of a request if the analyst is uncertain whether a request for an audit trail extract must be returned to the authorizing manager for resubmitting to TIGTA.

10.8.34.7.3.2.1.2
(04-10-2025)

Non-UNAX/Non-Criminally Related Activity Audit Trail Extract Requests

- (1) Authorizing managers and USRs must submit all requests for audit trails to support work related activities, employee integrity issues, and security concerns to a Cybersecurity IDRS security analyst for review and processing.
- (2) Requests for extracts of audit trails must be sent to an IDRS security analyst who is responsible for the databases where the access(es) or activities occurred. Cybersecurity IDRS security analysts must screen requests to ensure the requests apply to the analyst's IRS campus IDRS database. Requests that apply to another campus' database must be forwarded to the appropriate Cybersecurity IDRS security analyst for processing.
- (3) The Cybersecurity IDRS security analyst must screen all requests for extracts of audit trails to determine if the purpose of the request is to follow-up on a questionable access reported as an error by the employee or for a noncriminal activity.
 - a. For questionable accesses other than a reported error, the Cybersecurity IDRS security analyst must return the request to the originator and advise the originator to send the request directly to the local TIGTA.
 - b. The Cybersecurity IDRS security analyst must also advise the local TIGTA staff of the pending request.
- (4) When a request for an audit trail extract is to support work-related activities, employee integrity issues, or security concerns, the Cybersecurity IDRS security analyst must either have the requests processed internally via SAAS or send the request to a Computing Center IDRS security analyst using the required procedures.
- (5) Audit trail extracts cannot be used for performance evaluations.

10.8.34.7.3.2.1.3
(04-10-2025)

**Freedom of Information
Act Audit Trail Extract
Requests**

- (1) Authorizing managers and USRs must submit all requests for information under FOIA to a Cybersecurity IDRS security analyst who support the Andover campus domain for review and processing.
- (2) Cybersecurity IDRS security analysts who support the Andover campus domain (and/or the analyst's manager) must coordinate with the submitting disclosure officer to determine the necessary requirements to satisfy the requests.
- (3) Staff are to maintain a record of the personnel time (hours) and effort necessary to satisfy the FOIA request
 - a. If the FOIA request involves the effort of non-Cybersecurity Operations staff, the non-Cybersecurity Operations staff are to maintain a record of the actual personnel time (hours) and effort necessary to satisfy the FOIA request. Information on the actual personnel time and effort required must be provided to the disclosure officer along with the result of the request.
 - b. If the FOIA request can be completed in a timely and cost-efficient manner using SAAS, Cybersecurity IDRS security analysts who support the Andover campus domain (and/or the analyst's manager) and the disclosure officer must determine whether SAAS should be used to respond to the request.
 - c. It is the responsibility of the disclosure officer to determine the actual cost to the taxpayer and receive payment from the taxpayer for any FOIA information.
- (4) The Cybersecurity IDRS security analyst must include a statement to the disclosure officer with the results of the audit trail that "While information contained in the attached IDRS audit trail extract may be releasable, IDRS audit trails are an integral component of SACS. Therefore, the actual attachment, as presented, must not be released to the requesting taxpayer. Additional screening of the information contained in the report by the business function involved is mandatory."

10.8.34.7.3.2.1.4
(04-10-2025)

**Electronic Discovery
Requests**

- (1) All Electronic Discovery related requests for extracts of audit trails must be submitted to designated Cybersecurity IDRS security analysts in accordance with established Electronic Discovery Request procedures.
- (2) Form 9936 must not be used for any Electronic Discovery related requests for extracts of audit trails.

10.8.34.7.3.2.2
(04-10-2025)

**Requesting Audit Trail
Extracts**

- (2) Managers/USRs must submit all audit trail requests on Form 9936 which is signed by the requestor (group manager or USR) and the approving manager at the next higher level. The Form 9936 must be submitted to the manager's or USR's home campus Cybersecurity IDRS security analyst and must contain

#

#

#

the specific information and instructions for the search criteria including dates, SSN, command codes, etc. The form may be electronically sent to the Cybersecurity IDRS security analyst via secured email. Valid PDF digital signatures are acceptable. Otherwise, the form may be faxed or mailed to the Cybersecurity IDRS security analyst. Faxing of forms must adhere to procedures for faxing sensitive information but do not need to be followed-up with the original copy.

- (3) Upon receipt of Form 9936, Cybersecurity IDRS security analysts may forward the request to the computing center Cybersecurity Operations staff for processing or process the request using the SAAS Application.

10.8.34.7.3.2.2.1
(04-10-2025)
**Processing of Audit Trail
Extracts by the
Cybersecurity
Computing Center
Operations Staff (IAP
IDRS Audit Trail
Extracts)**

- (1) Upon receipt of Form 9936, and the determination that the request is appropriate, the Cybersecurity IDRS security analyst submits the form to a computing center IDRS security analyst in accordance with current procedures for processing. If it is necessary for the Cybersecurity IDRS security analyst to open a help desk ticket for the audit trail request, no details, such as name or SSN are given to the help desk.
- (2) The computing center IDRS security analyst must log all audit trail extract requests and process in accordance with current procedure.
- (3) Upon completion of the audit trail extract job, the computing center IDRS security analyst or computer systems analyst (CSA) must verify output of the audit trail extract job, notify the Cybersecurity IDRS security analyst that the request has been completed, and provide the job name and number of the audit trail output. The job must be loaded on Control-D web for retrieval by the Cybersecurity IDRS security analyst.
- (4) The Cybersecurity IDRS security analyst receives the audit trail output extract, validates that the appropriate search criteria were used and transmits the extract to the original requestor in a secure manner. The extract may be electronically sent to the requestor via secured email.
- (5) Requestors of an audit trail extract must contact the requestor's Cybersecurity IDRS security analyst if the requestor has any questions about the items contained in the extract.
- (6) For information regarding the IAP audit trail format, refer to Exhibit 10.8.34-17, IDRS Audit Trail Record Format – ICS/ACS/Print (IAP).

10.8.34.7.3.2.2.2
(04-10-2025)
**Processing Audit Trail
Extracts using the SAAS
Application (SAAS IDRS
Audit Trail Extracts)**

- (1) Upon receipt of Form 9936, and the determination that the request is appropriate, Cybersecurity IDRS security analysts (at the discretion of Cybersecurity Operations management) have the option of requesting IDRS audit trail extracts via the SAAS instead of forwarding the request to the computing center Cybersecurity Operations staff for processing.
- (2) The Cybersecurity IDRS security analyst must log all audit trail extract requests and process requests using the SAAS IDRS security specialist module in accordance with current procedure.
- (3) Upon completion of the audit trail extract job, the Cybersecurity IDRS security analyst must verify output of the audit trail extract job and transmit the extract to the requestor in a secure manner. The extract may be electronically sent to

the requestor via secured email. The computing center IDRS security analyst must log all audit trail extract requests and process in accordance with current procedure.

- (4) Requestors of an audit trail extract must contact the requestor's Cybersecurity IDRS security analyst if the requestor has any questions about the items contained in the extract.
- (5) For information regarding the SAAS audit trail format, refer to Exhibit 10.8.34-16, IDRS Audit Trail Record Format – Security Audit and Analysis System (SAAS).

This Page Intentionally Left Blank

Exhibit 10.8.34-1 (04-10-2025)**Terms and Acronyms**

Term	Definition or Description
Account	A tax record. Tax data is identified by SSN or by employer identification number (EIN).
Account Management Services (AMS)	AMS is a web-based system that emphasizes the sharing of key business data and provides a consolidated and synchronized view of taxpayer data and contact information from various IRS systems, moving organizations towards an integrated desktop.
ACS	Automated Collection System
Adjustment	A change to what was originally input or posted to an account on IDRS. Usually caused by performing additional research of an account, taxpayer contact or receipt of additional correspondence.
AMS	Account Management Services
AO	Authorizing Official
Audit Information Management System (AIMS)	Audit Information Management System (AIMS) provides inventory and activity controls of active Examination cases. It uses linkage to IDRS to input status changes, adjustments, and case closing actions. Note: This system is not a part of IDRS and is outside the boundary of the IDRS application for purposes of the IDRS investment definition (E300, FISMA/IT Security).
Audit Trail	An electronic record of all actions taken on IDRS.
Authorizing Official (AO)	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Accountable for the security risks associated with information system operations.
Automated Collection System (ACS)	Provides inventory of delinquent taxpayers.
BEARS	Business Entitlement Access Request System
BI	Background Investigation
BOD	Business Operating Division
BMF	Business Masterfile

Exhibit 10.8.34-1 (Cont. 1) (04-10-2025)**Terms and Acronyms**

Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, UNAX, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for other than an authorized purpose (i.e., a purpose unrelated to their official duties/functions) (Treasury Incident Response Plan (IRP)). Note: A breach is a type of incident that involves personally identifiable information (PII).
Business Master-file Case Creation Non-Filer Identification Process (BMF CCNIP)	An application and database which has the ability to interactively identify, prioritize and select business non-filer tax delinquency cases using third party data secured.
CCNIP	Case Creation Non-Filer Identification Process
CFOL	Corporate Files On-Line
CISA	Cybersecurity and Infrastructure Security Agency
CMMI	Capability Maturity Model Integration
CSA	Computer Systems Analyst
Data	Facts and statistics collected together for reference or analysis. Note: For example, in processing individual income tax returns, that group of facts peculiar to a particular taxpayer.
Database	A database is an organized grouping of data to fit the information needs of multiple functions of an organization. The database can be manipulated through an online real-time system. A database is accessed by using a command code.
EAD	Effective Action Date
ECC	Enterprise Computing Center
ECC-MEM	Enterprise Computing Center - Memphis
ECC-MTB	Enterprise Computing Center - Martinsburg
EFC	Enterprise FISMA Compliance
ELC	Enterprise Life Cycle
EIN	Employer Identification Number
Employer Identification Number (EIN)	A nine-digit number, also referred to as the EIN, used to identify business taxpayers on the Business Master File. The first two digits represent the district office code.
Entity	The portion of the master file record which identifies the taxpayer. It contains the name, address and SSN or EIN.

Exhibit 10.8.34-1 (Cont. 2) (04-10-2025)

Terms and Acronyms

EO	Executive Order
EOD	Enter on Duty
EOPS	IRS IT, Enterprise Operations
ERS	Error Resolution System
ESRF	Employee Security Record File
File	A file is a collection of related records. However, unlike a database, the file does not have to be organized. Normally files are not accessible unless a real-time program organizes the data.
File Source	A one-digit code which follows the TIN.
Federal Information Security Modernization Act (FISMA)	Federal Information Security Management Act (FISMA) - Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
FISMA	Federal Information Security Modernization Act
FMSS	Facilities Management and Security Services
FOIA	Freedom of Information Act
Generalized Unpostable Framework (GUF)	The Generalized Unpostable Framework (GUF) system establishes an inventory of transactions that could not post to the master file and provides programs to correct the transactions. GUF controls, validates, and corrects transactions through Generalized Mainline Framework (GMF).
GMF	Generalized Mainline Framework
GUF	Generalized Unpostable Framework
HRConnect	HRConnect is a web-based application that enables HR professionals, managers, and employees to manage HR processes efficiently and easily within their organization.
IAP	ICS/ACS/Print
IBM	International Business Machines
ICS	Integrated Collection System
IDRS	Integrated Data Retrieval System
IDRS Online Reports Services (IORS)	IORS is a web-based database management application supporting the security office of the IRS. It provides IDRS security personnel and IRS managers with online access to various IDRS security reports and forms. Note: The IORS system is not a part of IDRS and is outside the boundary of the IDRS application for purposes of the IDRS investment definition (E300, FISMA/IT Security).

Exhibit 10.8.34-1 (Cont. 3) (04-10-2025)**Terms and Acronyms**

IDRS Unit and USR Database (IUUD)	<p>IUUD allows IRS employees and managers who use IDRS and have intranet access to get contact information about IDRS units, managers and security personnel. For each IDRS unit, the IUUD enables users to find the USR's name and phone number, the manager's name, address and phone number, a description of the unit and additional information.</p> <p>Note: IUUD is not a part of IDRS and is outside the boundary of the IDRS application for purposes of the IDRS investment definition (E300, FISMA/IT Security).</p>
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
Integrated Collection System (ICS)	Allows agents to access extracted IDRS data.
Integrated Data Retrieval System (IDRS)	<p>The Integrated Data Retrieval System (IDRS) provides access to online taxpayer account research and is a major application supported on the Unisys and IBM mainframes at the ECC Martinsburg and ECC Memphis campuses and controlled through the Security and Communication System (SACS).</p> <p>Note: IDRS is a mission critical steady state system consisting of databases and operating programs that support IRS employees working active tax cases within each business function across the entire IRS. This system manages data that was extracted from the Corporate Account Data Stores (Business Master File (BMF), EPMF, IMF and CADE) allowing IRS employees to take specific actions on taxpayer account issues, track status and post transaction updates back to the Master Files. It provides for systemic review of case status and notice issuance based on case criteria, alleviating staffing needs and providing consistency in case control.</p>
IOIRS	IDRS Online Reports Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITM	Integrated Talent Management
IUUD	IDRS Unit and USR Database
LSS	Lean Six Sigma
LWOP	Leave Without Pay
MFE	Multifunctional Equipment
MFT	Master File Transaction

Exhibit 10.8.34-1 (Cont. 4) (04-10-2025)**Terms and Acronyms**

MPAF	Maximum Profile Authorization File
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OI	Office Identifiers
OMB	Office of Management and Budget
PIN	Personal Identification Number
PIV	Personal Identity Verification
PDS	Protection and Data Security
POC	Point Of Contact
SAAS	Security Audit and Analysis System
SACS	Security and Communications System
SB/SE	Small Business/Self-Employed
SBU	Sensitive But Unclassified
Security Account Administrator	The IDRS security account administrator performs the user and unit account administration tasks.
Security Analyst	The IDRS security analyst performs the policy support and oversight tasks.
Security and Communication System (SACS)	Provides user and application security validation for access to IDRS, CFOL, and EFTP.
Security File	The IDRS file that contains, for security purposes, significant data concerning each user and each terminal in the system.
SEID	Standard Employee Identifier
SOP	Standard Operating Procedure
SOSD	Security Operations & Standards Division
SP	Special Publication
SPMO	Security Program Management Office
SRM	Security Risk Management
SSN	Social Security Number
TAPS	Totally Automated Personnel System
Tax Period	The period of time for which a return is filed. The Service uses a six-digit code to indicate the end of the tax period for a given return. (The first four digits represent the year, and the next two digits represent the month).
TD	Treasury Directive
TIGTA	Treasury Inspector General for Tax Administration

Exhibit 10.8.34-1 (Cont. 5) (04-10-2025)**Terms and Acronyms**

TIMIS	Treasury Integrated Management Information System
TIN	Taxpayer Identification Number
TRDB	Tax Return Database
TS	Taxpayer Services
TSA	Terminal Security Administrator
TSID	Terminal Security Identification
TVR	Terminal Vector Record
UCCP	Unit Command Code Profile
UNAX	Unauthorized Access
Unpostables	Data that cannot be posted (updated) to a master file such as an incorrect TIN, date, or transaction code.
User	A user is an employee, who uses terminals to update, change, correct or add data to various computer systems.
USGCB	United States Government Configuration Baseline
USR	Unit Security Representative
UWR	Unified Work Request

Exhibit 10.8.34-2 (04-10-2025)**Related Resources****IRS Publications**

- IRM 2.3, *Terminal Responses series*
- IRM 2.4, *Terminal Input series*
- IRM 2.9.1, *Integrated Data Retrieval System Procedures, Integrated Data Retrieval System*
- IRM 3.12.32, *Error Resolution – General Unpostables*
- IRM 6.751.1, *Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance*
- IRM 10.5.5, *Privacy and Information Protection, IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*
- IRM 10.5.7, *Privacy and Information Protection, Use of Pseudonyms by IRS Employees*
- IRM 10.5.8, *Privacy and Information Protection, Sensitive But Unclassified (SBU) Data Policy: Protection SBU in Non-Production Environments*
- IRM 10.8.1, *Information Technology (IT) Security, Security Policy*
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.9.1, *Classified National Security Information (CNSI)*
- IRM 10.23.3, *Personnel Security, Suitability for Employment and Personnel Security Operations*
- Document 12926-SA, *SACS Security Accounts Administrator Command Code Procedures*
- Document 12926-USR, *SACS Unit Security Representative Command Code Procedures*
- Document 12990, *Record Control Schedules (RCS)*
- Form 9936, *Request for Audit Trail Extract*
- Form 9937, *IDRS Unit Request*
- Form 9937-A, *IDRS Unit Request Continuation*
- Form 11370-A, *Recertification of UNAX Awareness Briefing*
- Form 13230, *IDRS Security Personnel Designation*
- Form 14665, *Sensitive But Unclassified (SBU) Data Use Request Form*

Department of the Treasury Publications

- TD P 85-01: Treasury Directive Publication 85-01 Version 3.1.3, “*Treasury Information Technology (IT) Security Program*,” issued February 28, 2022
- *Departmental Incident Response Plan (IRP)*, Revision 4.0, issued June 2023

National Institute of Standards and Technology (NIST) Publications

- NIST: SP 800-53: NIST Special Publication 800-53 Revision 5.1.1, “*Security and Privacy Controls for Information Systems and Organizations*,” issued November 7, 2023

Exhibit 10.8.34-3 (04-10-2025)
Distribution Procedures

#

[illegible][illegible]

#

##

#

--	--	--	--

#

#

[illegible][illegible]

#

[illegible][illegible]

#####

[illegible]

Exhibit 10.8.34-11 (04-10-2025)**IDRS Office Identifiers, Organization Code Ranges, and Unpostable Holding Units**

This exhibit defines the series of organization codes, IDRS OIs, and Unpostable Holding Units for use by IRS business divisions.

#

Exhibit 10.8.34-12 (04-10-2025)**IDRS Organization Codes — IRS Campuses**

This exhibit defines the series of organization codes for use by the IRS campuses. These offices have OIs from 01 to 10.

#

Exhibit 10.8.34-13 (04-10-2025)**IDRS Organization Codes - Taxpayer Services (TS) Area Offices**

This exhibit defines the series of organization codes for use by the TS area offices. These offices have Ols from 11 to 17.

#

Exhibit 10.8.34-14 (04-10-2025)**IDRS Organization Codes - Small Business/Self-Employed (SB/SE) Area Offices**

This exhibit defines the series of organization codes for use by the Small Business/ Self Employed (SB/SE) area offices. These offices have OIs from 21 to 27 and 35 except for SB/SE Communication, Liaison & Disclosure organization user accounts will remain in OI 79.

#

Exhibit 10.8.34-15 (04-10-2025)**IDRS Organization Codes - Other Business Divisions**

This exhibit defines the series of organization codes for use by the other IRS business divisions. These offices have Ols as follows: Appeals (66), SB/SE - Disclosure (79), Communication and Liaison (79), Counsel (69), Criminal Investigation (60), Large Business and International (50), Tax Exempt and Government Entities (40), and Taxpayer Advocate (63).

#

Exhibit 10.8.34-16 (04-10-2025)

IDRS Audit Trail Record Format — Security Audit and Analysis System (SAAS)

This exhibit describes the audit trail record format for audit trail extracts requested via SAAS.

#

Exhibit 10.8.34-17 (04-10-2025)**IDRS Audit Trail Record Format — ICS/ACS/Print (IAP)**

This exhibit describes the audit trail record format for audit trail extracts requested via IAP.

#

#####

#####

#

[illegible]

##

#####

[illegible]

#

#####

~~##~~
~~##~~
~~##~~

#

#

#

