



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.34

NOVEMBER 28, 2023

EFFECTIVE DATE

(11-28-2023)

PURPOSE

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

MATERIAL CHANGES

- (1) The following subsections have been updated to align with IRM 1.11.2, Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls:
 - Transferred Roles and Responsibilities from IRM 10.8.34.2 to IRM 10.8.34.1.3.
 - Transferred Risk Acceptance and Risk-Based Decisions from IRM 10.8.34.1.3 to IRM 10.8.34.4.
 - Created IRM 10.8.34.7 for IDRS Roles and Responsibilities.
 - Transferred IDRS Key Governance and Related Roles & Responsibilities from IRM 10.8.34.2.1 to IRM 10.8.34.7.1.
 - Transferred Senior Management/Executive from IRM 10.8.34.2.1.1 to IRM 10.8.34.7.1.1.
 - Transferred IDRS Security Program Office from IRM 10.8.34.2.1.2 to IRM 10.8.34.7.1.2.
 - Transferred Manager from IRM 10.8.34.2.1.3 to IRM 10.8.34.7.1.3.
 - Transferred Organization/Functional Roles and Responsibilities from IRM 10.8.34.2.2 to IRM 10.8.34.7.2.
 - Transferred IDRS Security Program Management Office from IRM 10.8.34.2.2.1 to IRM 10.8.34.7.2.1.
 - Transferred IDRS Security Business Division Point-Of-Contact from IRM 10.8.34.2.2.2 to IRM 10.8.34.7.2.2.
 - Transferred IRS Information Technology (IRS IT) Enterprise Operations, Security Operations & Standards Division (EOPS-SOSD) Management from IRM 10.8.34.2.2.3 to IRM 10.8.34.7.2.3.
 - Transferred IRS Information Technology (IRS IT) Enterprise Operations, Security Operations & Standards Division (EOPS-SOSD) Management from IRM 10.8.34.2.2.3 to IRM 10.8.34.7.2.3.
 - Transferred IRS Information Technology (IRS IT) Cybersecurity Operations Management from IRM 10.8.34.2.2.4 to IRM 10.8.34.7.2.4.
 - Transferred IDRS Security Account Administrator from IRM 10.8.34.2.2.5 to IRM 10.8.34.7.2.5.
 - Transferred Computing Center IDRS Security Administrator from IRM 10.8.34.2.2.6 to IRM 10.8.34.7.2.6.
 - Transferred IDRS Security Analyst from IRM 10.8.34.2.2.7 to IRM 10.8.34.7.2.7.
 - Transferred Campus IDRS Security Analyst from IRM 10.8.34.2.2.7.1 to IRM 10.8.34.7.2.7.1.
 - Transferred Computing Center IDRS Security Analyst from IRM 10.8.34.2.2.7.2 to IRM 10.8.34.7.2.7.2.
 - Transferred Unit Security Representative (USR) from IRM 10.8.34.2.2.8 to IRM 10.8.34.7.2.8.
 - Transferred Alternate USR from IRM 10.8.34.2.2.9 to IRM 10.8.34.7.2.9.
 - Transferred Terminal Security Administrator (TSA) from IRM 10.8.34.2.2.10 to IRM 10.8.34.7.2.10.
 - Transferred IORS Report Reviewer from IRM 10.8.34.2.2.11 to IRM 10.8.34.7.2.11.
 - Transferred IORS Primary Report Reviewer from IRM 10.8.34.2.2.11.1 to IRM 10.8.34.7.2.11.1.
 - Transferred IORS Secondary Report Reviewer from IRM 10.8.34.2.2.11.2 to IRM 10.8.34.3.2.11.2.
 - Transferred Integrated Data Retrieval System (IDRS) from IRM 10.8.34.1.4 to IRM 10.8.34.3.
 - Transferred IDRS Security System from IRM 10.8.34.1.5 to IRM 10.8.34.4.
 - Transferred IDRS Security System from IRM 10.8.34.1.6 to IRM 10.8.34.5.
 - Transferred Authorized Access from IRM 10.8.34.1.7 to IRM 10.8.34.6.
 - Created IRM 10.8.34.1.4 for Program Management and Review.

- Created IRM 10.8.24.1.5 for Program Controls.

(2) Editorial changes made throughout the IRM for clarity.

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, Policy and Guidance* and IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.

AUDIENCE

The provisions in the manual apply to:

- a) All offices and business, operating, and functional units within the IRS.
- b) Individuals 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 IRS information and information systems, which include IRS production, development, test, and contractor systems. For information systems that store, process, or transmit classified information, refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional procedures for protecting classified information.

Kaschit Pandya
Acting, 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	
10.8.34.4	IDRS Security System	#
10.8.34.5	Authorized Access	
10.8.34.6	Communications Protocol	
10.8.34.7	IDRS Roles and Responsibilities	
10.8.34.7.1	IDRS Key Governance and Related Roles & Responsibilities	
10.8.34.7.1.1	Senior Management/Executives	
10.8.34.7.1.2	IDRS Security Program Officer	
10.8.34.7.1.3	Manager	
10.8.34.7.2	Organization/Functional Roles and Responsibilities	
10.8.34.7.2.1	IDRS Security Program Management Office	
10.8.34.7.2.2	IDRS Security Business Division Point-of-Contact	
10.8.34.7.2.3	IRS Information Technology (IRS IT) Enterprise Operations, Security Operations & Standards Division (EOPS-SOSD) Management	
10.8.34.7.2.4	IRS Information Technology (IRS IT) Cybersecurity Operations Management	
10.8.34.7.2.5	IDRS Security Account Administrator	
10.8.34.7.2.6	Computing Center IDRS Security Administrator	
10.8.34.7.2.7	IDRS Security Analyst	
10.8.34.7.2.7.1	Campus IDRS Security Analyst	
10.8.34.7.2.8	Unit Security Representative (USR)	#
10.8.34.7.2.9	Alternate USR	
10.8.34.7.2.10	Terminal Security Administrator (TSA)	
10.8.34.7.2.11	IOIRS Report Reviewer	
10.8.34.7.2.11.1	IOIRS Primary Report Reviewer	
10.8.34.7.2.11.2	IOIRS Secondary Report Reviewer	

10.8.34.8	Management Controls	
10.8.34.8.1	Security Planning	
10.8.34.8.1.1	Rules of Behavior	
10.8.34.9	Operational Controls	
10.8.34.9.1	Security Awareness and Training	
10.8.34.9.1.1	Awareness	
10.8.34.9.1.1.1	IDRS User Security Awareness Training	
10.8.34.9.1.2	Training	
10.8.34.9.1.2.1	Manager Training	
10.8.34.9.1.2.2	IDRS Security Program Management Office Staff Training	
10.8.34.9.1.2.3	IDRS Security Analyst and Computing Center IDRS Security Analyst Training	
10.8.34.9.1.2.4	IDRS Security Account Administrator and Computing Center IDRS Security Administrator Training	
10.8.34.9.1.2.5	Unit Security Representative (USR) and Alternate USR Training	
10.8.34.9.1.2.5.1	Course Development and Revision	
10.8.34.9.1.2.5.2	Initial Training	
10.8.34.9.1.2.5.3	Annual Refresher Training	
10.8.34.9.1.2.5.4	Unit Security Representative Training Annual Compliance Review	
10.8.34.9.1.2.6	Terminal Security Administrator (TSA)	#
10.8.34.10	Technical Controls	
10.8.34.10.1	Identification and Authentication	
10.8.34.10.1.1	User Identification and Authentication	#
10.8.34.10.1.3	Workstation Identification and Authentication	#
10.8.34.10.1.3.2	Designation of Terminals	#
10.8.34.10.1.3.3	Location of Terminals	#
10.8.34.10.1.3.6	Terminal Shutdowns During Emergencies	#
10.8.34.10.2	Access Control	#

[illegible]

#

10.8.34.10.3 Audit and Accountability

10.8.34.10.3.1 IDRS Security Reports

10.8.34.10.3.1.1 IDRS Online Reports Services (IORS)

10.8.34.10.3.1.2 Review and Certification of Security Reports in IORS

10.8.34.10.3.1.2.1 Security Reports Requiring Certification by an IDRS Security Account Administrator

10.8.34.10.3.1.2.2 Security Reports Requiring Certification by an IDRS Security Analyst

10.8.34.10.3.1.2.3 Security Reports Requiring Certification by a Primary Report Reviewer

#

10.8.34.10.3.2.1 Audit Trail Extracts

10.8.34.10.3.2.1.1 UNAX Related and Suspected Criminal Activity Audit Trail Extract Requests

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

10.8.34.10.3.2.1.3 Freedom of Information Act Audit Trail Extract Requests

10.8.34.10.3.2.1.4 Electronic Discovery Requests

10.8.34.10.3.2.2 Requesting Audit Trail Extracts

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

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

Exhibits

- 10.8.34-1 Glossary
- 10.8.34-2 Terms and Acronyms
- 10.8.34-3 Related Resources
- 10.8.34-4 Distribution Procedures

#

- 10.8.34-12 IDRS Office Identifiers, Organization Code Ranges, and Unpostable Holding Units
- 10.8.34-13 IDRS Organization Codes — IRS Campuses
- 10.8.34-14 IDRS Organization Codes - Wage and Investment (W&I) Area Offices
- 10.8.34-15 IDRS Organization Codes - Small Business/Self-Employed (SB/SE) Area Offices
- 10.8.34-16 IDRS Organization Codes - Other Business Divisions
- 10.8.34-17 IDRS Audit Trail Record Format — Security Audit and Analysis System (SAAS)
- 10.8.34-18 IDRS Audit Trail Record Format — ICS/ACS/Print (IAP)

#

10.8.34.1
(11-28-2023)
**Program Scope and
Objectives**

- (1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security controls and guidance for the use of the Integrated Data Retrieval System (IDRS) within the Internal Revenue Service (IRS).
 - a. This manual is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IDRS.
- (2) **Purpose of the Program:** Develop and publish policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this manual apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals 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 IRS information and information systems, which include IRS production, development, test, and contractor systems. For information systems that store, process, or transmit classified information, refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional procedures for protecting classified information.
- (4) **Policy Owner:** Chief Information Officer
- (5) **Program Owner:** Cybersecurity, Threat Response and Remediation (an organization within Cybersecurity)
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.34.1.1
(11-21-2022)
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 Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.34.1.2
(11-21-2022)
Authority

- (1) All IRS systems and applications shall be compliant with Executive Orders (E.O.s), 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), The Department of the Treasury, and IRS guidelines as they apply.

10.8.34.1.3
(11-21-2022)
**Roles and
Responsibilities**

- (1) IRM 10.8.2, **Information Technology (IT) Security, IT Security Roles and Responsibilities**, defines IRS-wide roles and responsibilities related to IRS information and computer security and is the authoritative source for such information.

10.8.34.1.4
(11-28-2023)
**Program Management
and Review**

- (1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8.x series and the development of technology specific 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:
 - a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
 - b. To 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 to that IT resource.
 - c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), 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
(11-28-2023)
Program Controls

- (1) The provisions of this issuance are applicable to all individuals who use, manage users of, or support the security of the IDRS.
- (2) The IRS shall ensure that the product (e.g., software, hardware) and version selected is in accordance with IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) that dictates the official products and versions within the IRS.
- (3) The IRS shall ensure the application or system version is a version for which the vendor still offers standardized technical support.
- (4) IRM 10.8.34, *IDRS Security Controls*, shall be available to:
 - a. Individuals with responsibilities related to the security of IDRS.
 - b. Individuals who manage employees accessing IDRS.
 - c. Individuals responsible for development, testing, and maintenance of IDRS features.
 - d. Individuals with a need to know in Treasury Inspector General for Tax Administration (TIGTA).
- (5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive, or unless otherwise noted.
- (6) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.

#####

#

10.8.34.4
(11-21-2022)
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 shall be protected from unauthorized access, inspection, changes, and disclosure of any of the taxpayer's personal information and tax related information.
 - The IDRS user employee shall be protected from other personnel using personnel identification to access or make changes to an account.

10.8.34.5
(11-21-2022)
Authorized Access

- (1) IDRS users shall only access accounts necessary for accomplishing official duties.
- (2) IDRS user shall 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; and\
 - 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 shall 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 Unauthorized Access (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.

10.8.34.6
(11-21-2022)
**Communications
Protocol**

- (1) This section defines the communications protocol to be followed when addressing IDRS security issues.
- (2) Unless otherwise stated, the IDRS user shall direct IDRS security related concerns to the user's manager or Unit Security Representative (USR).
- (3) Unless otherwise stated, managers and USRs shall 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 Security Program Management Office. ,

- (4) Unless otherwise stated, the IDRS Security Account Administration staff and Cybersecurity IDRS Security Analysts shall elevate any IDRS security related concern the staff and Analysts are unable to resolve to the IDRS Security Program Management Office.
- (5) IDRS Security Business Division Points-Of-Contact (POCs) shall direct IDRS security related concerns to the IDRS Security Program Management Office 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 shall be elevated to the IDRS Security Program Management Office.
- (7) IDRS users, managers, or USRs rarely have a need to contact a Computing Center IDRS Security staff. Unless otherwise stated, any communication with Computing Center IDRS Security staff shall be routed through the IDRS Security Program Management Office.

10.8.34.7
(11-28-2023)
IDRS Roles and Responsibilities

- (1) The supplemental roles and responsibilities provided below are specific to the implementation of IDRS.

10.8.34.7.1
(11-21-2022)
IDRS Key Governance and Related Roles & Responsibilities

- (1) This section provides functional roles and responsibilities for personnel who have security-related governance responsibility for the protection information systems that the personnel operate, manage and support. These roles are defined in accordance with IRM 10.8.2.

10.8.34.7.1.1
(11-21-2022)
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 the IDRS Security.
- (3) Senior management/executives shall perform the following IDRS responsibilities:
 - a. Ensure IDRS Security policies and guidance are implemented.
 - b. Identify at least one individual as the 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 shall be provided to the IDRS Security Program Management Office.
 - c. Ensure 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, and IORS Security Report Reviewers.
 - e. Ensure the IDRS Security Account Administrators or the IDRS Security Program Management Office 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.
- i. Ensure that the required responses related to IDRS security report compliance are submitted timely to the IDRS Security Program Management Office 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 USR's or Alternate USR'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 the IRM.

10.8.34.7.1.2
(10-24-2011)

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.

10.8.34.7.1.3
(11-21-2022)

Manager

- (1) The manager of IDRS users shall be responsible for day-to-day implementation and administration of IDRS security.
- (2) The manager shall 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 Business Entitlement Access Request System (BEARS).

- i. Ensure questionable activity or potential UNAX violations are timely reported to TIGTA.
 - j. Report any IDRS user who refuses to certify or recertify the rules of behavior to employees' 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 shall 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 shall ensure the employee has met the recertification requirements, which includes having the employee review the UNAX briefing and signing the UNAX Recertification Certificate 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.
 - l. Fulfill any additional IDRS security responsibilities of the manager stated elsewhere in the IRM.
- (3) Managers who have been officially designated as the USR for the unit/group (via an approved Form 13230, *IDRS Security Personnel Designation*) shall 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.
- (5) Refer to IRM 10.8.2, for general policy related to the IT security role and responsibilities of the manager.

10.8.34.7.2
(10-14-2011)
**Organization/Functional
Roles and
Responsibilities**

- (1) This section provides functional roles and responsibilities for personnel who have IDRS security related responsibilities. These roles are defined in accordance with IRM 10.8.2.

10.8.34.7.2.1
(09-25-2020)
**IDRS Security Program
Management Office**

- (1) The IDRS Security Program Management Office is a function in the IRS Information Technology (IRS IT), Cybersecurity organization that was established to manage the IDRS Security Program.
- (2) The IDRS Security Program Management Office 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 Security Program Management Office activity.
 - c. IDRS Security Program Analyst(s) - individuals who support the day-to-day IDRS Security Program Management Office activity.
- (3) The IDRS Security Program Management Office shall 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.
 - 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, Unit Security Representatives, and business unit management. Any oversight and evaluation activities performed by or for the IDRS Security Program Management Office shall not substitute or replace any monitoring, training, or oversight activities required to be performed by IDRS Security Account Administrators, IDRS Security Analysts, Unit Security Representatives, or business unit management.
 - j. Support Cybersecurity staff in the review of requests to deviate from IDRS security policy stated in IRM 10.8.34, IDRS Security Controls.
 - k. Fulfill any additional IDRS security responsibilities of the IDRS Security Program Management Office stated elsewhere in the IRM.

10.8.34.7.2.2
(11-21-2022)

**IDRS Security Business
Division Point-of-
Contact**

- (1) 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) IDRS Security Business Division POC shall:
- a. Serve as the business organization's point of contact with the IDRS Security Program Management Office.
 - b. Serve as a liaison between the IDRS Security Program Management Office 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 IDRS 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 the 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.

#

sites/CyberAI-IDRSSecurity/SitePages/Home.aspx

10.8.34.7.2.3
(09-25-2020)
**IRS Information
Technology (IRS IT)
Enterprise Operations,
Security Operations &
Standards Division
(EOPS-SOSD)
Management**

- (1) IRS IT EOPS-SOSD Management shall assign security specialist(s) and/or security assistants as IDRS Security Account Administrators.
- (2) IRS IT EOPS-SOSD Management shall assign security specialist(s) and/or security assistants as Computing Center IDRS Security Administrators.

#

10.8.34.7.2.4
(09-25-2020)
**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.

#

#####

- (1) The IDRS Security Account Administrator performs tasks relating to the administration of IDRS user and unit accounts.
- (2) The IDRS Security Account Administrator shall be a non-bargaining unit employee who is a member of the EOPS-SOSD staff.
- (3) To help ensure proper separation of duties, the IDRS Security Account Administrator shall not simultaneously serve as Computing Center IDRS Security Administrator.

#

#####

[illegible]

10.8.34.7.2.6
(09-25-2020)

**Computing Center IDRS
Security Administrator**

- (1) The Computing Center IDRS Security Administrator performs tasks relating to the administration Computing Center IDRS security activity.
- (2) The Computing Center IDRS Security Administrator shall be a non-bargaining unit employee who is a member of the EOPS-SOSD staff.
- (3) To help ensure proper separation of duties, the Computing Center IDRS Security Administrator shall not simultaneously serve as IDRS Security Account Administrator.

10.8.34.7.2.7
(04-01-2014)

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.

10.8.34.7.2.7.1
(11-21-2022)

**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 shall be a non-bargaining unit employee who is a member of the Cybersecurity Operations staff.

[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 shall 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 shall be submitted to an IDRS Security Account Administrator on a Form 13230.
 - b. Before submission, the Form 13230 shall 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 shall 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 shall have a “completed” background investigation status.

- (5) The Alternate USR shall complete:
 - a. Initial USR training prior to performing USR duties.
 - b. Shall complete USR refresher training at least annually.
- (6) The Alternate USR's manager shall 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 shall be approved by the Alternate USR's primary USR to ensure 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 shall 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 shall fulfill any additional IDRS security responsibilities of the Alternate USR stated elsewhere in the IRM.

10.8.34.7.2.10

(11-21-2022)

**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 TSA is optional and the discretion of business organization management. 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 shall be approved by a second level manager or higher in the TSA's business organization. The designation shall be submitted to the IDRS Security Account Administration staff on Form 13230. Before submission, the Form 13230 shall 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 shall 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 shall 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 shall 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.

10.8.34.7.2.11
(11-21-2022)
IORS 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

10.8.34.7.2.11.1
(11-21-2022)
IORS 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 shall 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 shall have a designated IORS Primary Report Reviewer, who shall be submitted to the IDRS Security Account Administration staff on Form 13230. Before submission, the Form 13230 shall be coordinated with the primary USR(s) to ensure the primary USR(s) is aware of who is being designated as IORS Primary Report Reviewer.
- (4) The IDRS Security Account Administration staff shall 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 shall 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 shall 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 shall remove these permissions when they are no longer needed.
- (10) IORS Primary Report Reviewer shall fulfill any additional IDRS security responsibilities of the IORS Primary Report Reviewer stated elsewhere in the IRM.

10.8.34.7.2.11.2
(04-01-2014)

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 an unit where the Primary Report Reviewer role is being performed by another individual.
- (3) The IORS Secondary Report Reviewer shall 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 shall 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 the IRM.

10.8.34.8
(11-21-2022)

Management Controls

- (1) Per IRM 10.8.1, IRS shall 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 shall be implemented in accordance with IRM 10.8.1:
 - CA - Security Assessment and Authorization (SA & A)
 - PL - Security Planning
 - RA - Risk Assessment
 - SA - System and Service Acquisition
 - SR - Supply Chain Risk Management

10.8.34.8.1
(09-25-2020)
Security Planning

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

10.8.34.8.1.1
(11-21-2022)
Rules of Behavior

- (1) IDRS users shall sign a statement acknowledging that they have read and understand the rules of behavior.
- (2) The BEARS system shall be used to document IDRS users' acknowledgement they have read and understand the rules of behavior.
 - a. Prior to being added to IDRS, users shall sign the BEARS rules of behavior statement acknowledging that they have read and understand the rules.
 - b. To maintain access privileges, IDRS users shall 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.

10.8.34.9
(11-21-2022)
Operational Controls

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

10.8.34.9.1
(09-25-2020)
Security Awareness and Training

- (1) Per IRM 10.8.1, the IRS shall develop and implement an IDRS IT security awareness and training program.

10.8.34.9.1.1
(10-14-2011)
Awareness

- (1) IRM 10.8.1 requires system users to complete security awareness training when being granted access to a system and annually for as long as they remain system users. This IRM further defines security awareness training requirements as they pertain to IDRS security.

10.8.34.9.1.2.4
(11-21-2022)

**IDRS Security Account
Administrator and
Computing Center IDRS
Security Administrator
Training**

- (1) IRS IT EOPS-SOSD management shall ensure IDRS Security Account Administrators and Computing Center IDRS Security Administrators are properly trained to perform IDRS Security related tasks.

10.8.34.9.1.2.5
(09-25-2020)

**Unit Security
Representative (USR)
and Alternate USR
Training**

- (1) Employees designated as USR or Alternate USR shall complete the required initial and annual refresher training.

#

10.8.34.9.1.2.5.1
(11-21-2022)

**Course Development
and Revision**

- (1) The IDRS Security Program Management Office shall be responsible for developing and revising the required USR initial and annual refresher training.
 - a. The IDRS Security Program Management Office shall develop the required USR initial and annual refresher training courses and ensure the courses are available on the ITM system.
 - b. The IDRS Security Program Management Office shall 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 Security Program Management Office shall contact the IRS IT Learning & Education staff each year to notify staff if any course revisions are necessary.
 - d. The IDRS Security Program Management Office shall update the required USR initial and annual refresher training courses as necessary.

10.8.34.9.1.2.5.2
(11-21-2022)

Initial Training

- (1) Employees designated as USR or Alternate USR shall complete the ITM — IDRS USR Training.
 - a. Security command codes shall not be placed in the profiles any USR or Alternate USR who has not completed this ITM course.
 - b. Security command codes shall 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 thru June 30.

- (2) New USRs and Alternate USRs shall 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 shall be considered new and are required to complete the initial training course before security command codes are added to the USR's profile.

10.8.34.9.1.2.5.3
(09-25-2020)
**Annual Refresher
Training**

- (4) IDRS Security Account Administration staff shall remove security command codes from the profile of any USR or Alternate USR who received the command without completing the required initial training.

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

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

- (3) Security command codes shall 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 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 shall 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 Security Program Management Office shall send an e-mail message to USRs and Alternate USRs each year when the annual refresher training course is available on the ITM system.
 - a. The message shall inform USRs and Alternate USRs the training is available.
 - b. The message shall inform USRs and Alternate USRs of the date by which the training is to be completed.
 - c. The message shall advise USRs and Alternate USRs that the training is mandatory.
 - d. The message shall be sent to every employee who has been designated as a current USR or Alternate USR in the IDRS Unit & USR Database (IUUD).
 - e. The message shall be sent to the USR/Alternate USR's official e-mail address that appears in the Discovery Directory database.

10.8.34.9.1.2.5.4
(11-21-2022)
**Unit Security
Representative Training
Annual Compliance
Review**

- (1) The IDRS Security Program Management Office shall 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 Security Program Management Office shall perform a compliance check to identify USRs and Alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS Security Program Management Office shall obtain an ITM listing of USRs and Alternate USRs who have completed the required training.

- b. The IDRS Security Program Management Office shall use the ITM listing to identify USRs and Alternate USRs who have not completed the required training.
 - c. The IDRS Security Program Management Office shall send an e-mail 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 Security Program Management Office shall perform a compliance check to identify USRs and Alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS Security Program Management Office shall obtain an ITM listing of USRs and Alternate USRs who have completed the required training.
 - b. The IDRS Security Program Management Office shall use the ITM listing to identify USRs and Alternate USRs who have not completed the required training.
 - c. The IDRS Security Program Management Office shall send an e-mail 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 e-mail message shall 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 Security Program Management Office shall perform a compliance check to identify USRs and Alternate USRs who have not completed the required initial and annual refresher training.
 - a. The IDRS Security Program Management Office shall obtain an ITM listing of USRs and Alternate USRs who have completed the training as required.
 - b. The IDRS Security Program Management Office shall use the ITM listing to identify USRs and Alternate USRs who have not completed the training as required.
 - c. The IDRS Security Program Management Office shall send an e-mail 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 e-mail message shall 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 Security Program Management Office shall 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 work days after the end of the FISMA training year, the IDRS Security Program Management Office shall 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 Security Program Management Office shall obtain an ITM listing of USRs and Alternate USRs who have completed the training as required.
 - b. The IDRS Security Program Management Office shall use the ITM listing to identify USRs and Alternate USRs who have not completed the training as required.
 - c. The IDRS Security Program Management Office shall send an e-mail 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 7 calendar days after completing its annual compliance review, the IDRS Security Program Management Office shall 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 shall 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 shall 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 shall 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 shall send the IDRS Security Program Management Office a list of the USRs and Alternate USRs whose security command codes were removed.
 - f. The IDRS Security Account Administration staff shall 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 shall 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 Security Program Management Office may conduct additional compliance checks and/or send additional reminder messages to help increase compliance with USR training requirements.

10.8.34.9.1.2.6
(10-14-2011)

**Terminal Security
Administrator (TSA)**

- (1) The USR shall ensure the TSA has been trained on the following before performing TSA duties:
 - a. When and how to unlock IDRS terminals.

- ##

##

##

[illegible]

#

#####

[illegible][illegible]

Location of Terminals

- [illegible]

Note: Emergency closings may also include drills and exercises.

##

#

##

[illegible]

10.8.34.10.2
(09-25-2020)
Access Control

- (1) Per IRM 10.8.1, IRS shall implement access control measures that shall provide protection from unauthorized alteration, loss, unavailability, or disclosure of information. Access control shall 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]

##

**# # # # #

#**

[illegible]

#

#

[illegible]

#

##

#

#

#

##

#

#

#

```
# # # # #  
# # #  
  
# # # #  
# # #  
  
# # # # #  
# # # # #  
# # # # #  
# # # # #  
# # #  
  
# # # # #  
# # # # #  
# # # # #
```


#

[illegible]

##

#

[illegible]

#

#

10.8.34.10.2.4
(10-14-2011)

#

10.8.34.10.2.5
(11-21-2022)

#

10.8.34.10.3
(03-21-2019)

Audit and Accountability

- (1) Per IRM 10.8.1, the IRS shall 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 section defines audit and accountability requirements as they pertain to IDRS security.

10.8.34.10.3.1
(11-21-2022)

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 shall 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 shall refer the case and findings to the proper management or TIGTA officials.
- (3) IDRS Security personnel shall ensure any IDRS user found not to be following proper security measures (based on examination of the security reports, audit trail, etc.) shall 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 e-mail for oversight review.
- (5) The reviewer of an IDRS security report shall be independent. Reviewers shall not be the reviewer of the reviewer's own transactions.

10.8.34.10.3.1.1
(11-21-2022)

IDRS Online Reports Services (IORS)

- (1) In January 2004, the IDRS Online Reports Services (IORS) application became 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 Points-of Contact, 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 shall be protected.
 - c. Report data that is saved electronically shall be encrypted.
 - d. Report data that is printed, prints shall be stored in a secured location.
 - e. Report data transmitted via e-mail shall be transmitted using secured e-mail.
- (8) IORS uses the information from the IDRS Unit and USR Database to identify users who have been designated as Primary Report Reviewers for one or more IDRS units.
- (9) Business organizations shall ensure all IDRS units have properly designated Primary Report Reviewers. IDRS Security Account Administrators shall 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 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 shall 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 concern identified in the IDRS security reports.
- (11) The IORS application shall be the official retention of security reports. IORS shall retain security reports for a period of six years.

10.8.34.10.3.1.2
(11-21-2022)

**Review and Certification
of Security Reports in
IORS**

- (1) IDRS Security reports shall be reviewed in a timely and complete manner to help ensure users are working within required tax administration authorities. The review of security reports is important for detecting illegal or improper activities by the IDRS user. Any questionable transactions or activities shall be reviewed or turned over to the proper authorities for full investigations.
- (2) For business organizations, only the IORS Primary Report Reviewer for the unit shall certify that the security report has been reviewed and the necessary follow-up actions taken. However, Primary Report Reviewers can base certifications on the work of other users who have reviewed the security reports.
- (3) For business organizations either a USR, Alternate USR, manager, or a coordinator may be designated as the IORS Primary Report Reviewer for an IDRS unit. The Primary Report Reviewer is responsible for reporting actions taking on the security report and certifying that required activities were performed. When the Primary Report Reviewer is different from the manager, the manager is still held accountable for ensuring that all activities were performed as required.
- (4) The IORS application will maintain a record of all certifications by the Primary Report Reviewer for each report requiring certification and for each IDRS unit under the Primary Report Reviewer's responsibility.

#

- (6) Business organizations shall achieve at least a 90% certification rate for security reports.
- (7) IORS will retain a record of all certifications and associated comments as required in Document 12990, Records Control Schedule (RCS) 29, Item 283.

#

#####

- (1) The following daily security reports shall 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 shall 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 shall 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 shall certify these reports within 7 calendar days for the certification to be considered timely.
- (6) IORS will provide a reminder notification on the 5th 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.
- (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.

10.8.34.10.3.1.2.2
(10-14-2011)

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

- (1) The following daily security reports shall 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 Agency Wide Shared Services Labor Relations Office responsible for the accessing employee's business division. All accesses shall be sent to the appropriate Labor Relations Office within five calendar days of the transaction occurrences.
 - b. Report attempted or actual access to own or own spouse/ex-spouse tax accounts by TIGTA IDRS users shall be reported to TIGTA SIID (Special Inquiries and Intelligence Division).
- (3) IDRS Security Analysts are encouraged to review this report as they become available but shall certify the report within 7 calendar days for the certification to be considered timely.
- (4) IORS will provide a reminder notification on the 5th 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.

Security Reports Requiring Certification by a Primary Report Reviewer

- #####

- (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 shall 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 EOPS-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. Secondary and Primary 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.

#

#

10.8.34.10.3.2.1
(09-25-2020)

Audit Trail Extracts

- (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), shall be submitted to an IDRS Security Analyst for review and processing.
- (3) Refer to Requesting Audit Trail Extracts section within this IRM for how to request an audit trail extract.

10.8.34.10.3.2.1.1
(11-21-2022)

**UNAX Related and
Suspected Criminal
Activity Audit Trail
Extract Requests**

- (1) Managers shall 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 shall 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 shall perform extracts of audit trails when the reasons for the requests are to support the review of potential unauthorized accesses 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 shall 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 an unauthorized access.
 - 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 shall 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 shall contact the IDRS Security Program Management Office for determination on the appropriate routing of a request if the Analyst is uncertain whether a request for an audit trail extract shall be returned to the authorizing manager for resubmitting to TIGTA.

10.8.34.10.3.2.1.2
(11-21-2022)
**Non-UNAX/Non-
Criminally Related
Activity Audit Trail
Extract Requests**

- (1) Authorizing managers and USRs shall submit all requests for audit trails to support work related activities, employee integrity issues, security concerns to a Cybersecurity IDRS Security Analyst for review and processing.
- (2) Requests for extracts of audit trails shall be sent to an IDRS Security Analyst who is responsible for the databases where the access(es) or activities occurred. Cybersecurity IDRS Security Analysts shall screen requests to ensure the requests apply to the Analyst's IRS Campus IDRS database. Requests that apply to another campus' database shall be forwarded to the appropriate Cybersecurity IDRS Security Analyst for processing.
- (3) The Cybersecurity IDRS Security Analyst shall 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 shall 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 shall 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 shall 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.

10.8.34.10.3.2.1.3
(11-21-2022)

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

- (1) Authorizing managers and USRs shall submit all requests for information under the Freedom of Information Act 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) shall 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 shall 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 shall 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 shall 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, shall not be released to the requesting taxpayer. Additional screening of the information contained in the report by the business function involved is mandatory."

10.8.34.10.3.2.1.4
(09-25-2020)

**Electronic Discovery
Requests**

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

10.8.34.10.3.2.2

(11-21-2022)

**Requesting Audit Trail
Extracts**

- (2) Managers/ USRs shall submit all audit trail requests on an Audit Trail Extract Request Form 9936 which is signed by the requestor (group manager or USR) and the approving manager at the next higher level. The Form 9936 shall be submitted to the Manager's or USR's home campus Cybersecurity IDRS Security Analyst and shall 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 e-mail. Valid PDF digital signatures are acceptable. Otherwise, the form may be faxed or mailed to the Cybersecurity IDRS Security Analyst. Fax forms shall 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 Cybersecurity Computing Center Operations staff for processing, or process the request using the SAAS Application.

10.8.34.10.3.2.2.1

(11-21-2022)

**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 KISAM 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 shall 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) shall 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 shall 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 was used and transmits the extract to the original requestor in a secure manner. The extract may be electronically sent to the requestor via secured e-mail.
- (5) Requestors of an audit trail extract shall 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 10.8.34-18.

10.8.34.10.3.2.2.2
(11-21-2022)

**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 Security Audit and Analysis System (SAAS) instead of forwarding the request to the Cybersecurity Computing Center Operations staff for processing.
- (2) The Cybersecurity IDRS Security Analyst shall 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 shall 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 secure e-mail. The Computing Center IDRS Security Analyst shall log all audit trail extract requests and process in accordance with current procedure.
- (4) Requestors of an audit trail extract shall 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 10.8.34-17.

Exhibit 10.8.34-1 (11-21-2022)**Glossary****A**

Account - A tax record. Tax Data is identified by Social Security number (SSA) or by Employer Identification number (EIN).

Account Management Services - 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.

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.

Audit Information Management System (AIMS) - Audit Information Management System (AIMS) provides inventory and activity controls of active Examination cases. It uses linkage to Integrated Data Retrieval System (IDRS) to input status changes, adjustments, and case closing actions.

#

Audit Trail - An electronic record of all actions taken on IDRS.

Authorizing Official - 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. Previously known as the Designated Approving Authority.

B

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, 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 authorized purpose (i.e., a purpose unrelated to their official duties/functions) (Treasury IR Plan).

Note: A breach is a type of incident that involves PII.

Business Masterfile Case Creation Notice Identification Process (BMF CCNIP) - An application and database which has the ability to interactively identify, prioritize and select business Nonfiler tax delinquency cases using third party data secured.

C

Campus IDRS Security Officer - The Campus IDRS Security Officer role no longer exists. In 2009, to help ensure proper separation of duties, IDRS security user and unit account administration migrated from Cybersecurity Operations to the Enterprise Operations, Operational Security Program Management Office (EOPS-OSPMO). Cybersecurity Operations shall continue to perform IDRS security policy support and oversight related tasks. The IDRS Security Officer role has been replaced with two new roles: a. The IDRS Security Account Administrator performs the user and unit account administration tasks previously performed by the IDRS Security Officer. b. The IDRS Security Analyst performs the policy support and oversight tasks previously performed by the IDRS Security Officer.

D

Data - facts and statistics collected together for reference or analysis.

Exhibit 10.8.34-1 (Cont. 1) (11-21-2022)**Glossary**

Note: For example, in processing individual income tax returns, that group of facts peculiar to a particular taxpayer.

Database - A data base is an organized grouping of data to fit the information needs of multiple functions of an organization. The data base can be manipulated through an on-line real-time system. A data base is accessed by using a command code.

Dummy Module - A TIF account tax module that has not been fully updated from master file or is not at master file. It contains name control, TIN, MFT and tax period and will be replaced by the true tax module when the generated TC 902 finds a match on the Master File.

E

Employer Identification Number - A nine-digit number, also referred to as the EI number, 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.

Entity Index - An index of all entity modules at a given service center, used by ISRP when inputting returns and updated periodically by the centers.

Entity Module - Is that portion of the master file record which identifies the taxpayer. The entity module contains the taxpayer's name, address, Social Security or Employer Identification number, employment code if applicable, name control, location codes, filing requirement codes, tax period, and date of establishment. In the case of IMF it also includes filing status, spouse's name and social security number. This can also be a dummy module.

F

File - A file is a collection of related records. However, unlike a data base, 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 Taxpayer Identification Number (TIN).

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.

G

Generalized Unpostable Framework - 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).

I

IDRS - The Integrated Data Retrieval System (IDRS) is a major application supported on the Unisys and IBM mainframes at the ECC Martinsburg and ECC Memphis and controlled through the Security and Communication System (SACS).

Exhibit 10.8.34-1 (Cont. 2) (11-21-2022)**Glossary**#

#

IDRS Online Reports Services - IORS is a web-based database management application supporting the Security Office of the IRS. It provides IDRS security personnel and IRS managers with on-line access to various IDRS security reports and forms.

#

IDRS Unit and USR Database (IUUD) - IUUD allows IRS employees and managers who use the Integrated Data Retrieval System (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 Unit Security Representative's (USR) name and phone number, the manager's name, address and phone number, a description of the unit and additional information.

#

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.

S

Security File - The IDRS file that contains, for security purposes, significant data concerning each user and each terminal in the system.

T

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).

U

Unpostables - Data that cannot be posted (updated) to a master file such as an incorrect TIN, date, or transaction code.

User - Users are employees, who use terminals to update, change, correct or add data to various computer systems.

Exhibit 10.8.34-2 (11-21-2022)**Terms and Acronyms**

Following is a list of acronyms used in this IRM.

Acronym	Definition
AMS	Account Management Services
AO	Authorizing Official
BEARS	Business Entitlement Access Request System
BI	Background Investigation
BOD	Business Operating Division
CFOL	Corporate Files On-Line
CSA	Computer Systems Analyst
EAD	Effective Action Date
ECC	Enterprise Computing Center
ECC-MEM	Enterprise Computing Center- Memphis
ECC-MTB	Enterprise Computing Center - Martinsburg
EIN	Employer Identification Number
EOD	Enter on Duty
EOPS	IRS IT, Enterprise Operations
EOPS-SOSD	EOPS, Security Operations & Standards Division
ERS	Error Resolution System
ESRF	Employee Security Record File
FISMA	Federal Information Security Management Act
FMSS	Facilities Management and Security Services
FOIA	Freedom of Information Act
GUF	Generalized Unpostable Framework
IAP	ICS/ACS/Print
IBM	International Business Machines
IDRS	Integrated Data Retrieval System
IORS	IDRS Online Reports Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology

Exhibit 10.8.34-2 (Cont. 1) (11-21-2022)**Terms and Acronyms**

ITM	Integrated Talent Management
IUUD	IDRS Unit and USR Database
LWOP	Leave Without Pay
MFE	Multifunctional Equipment
MFT	Master File Transaction
MPAF	Maximum Profile Authorization File
NIST	National Institute of Standards and Technology
OI	Office Identifiers
OMB	Office of Management and Budget
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
SEID	Standard Employee Identifier
SOP	Standard Operating Procedure
SSN	Social Security Number
TAPS	Totally Automated Personnel System
TD	Treasury Directive
TIGTA	Treasury Inspector General for Tax Administration
TIMIS	Treasury Integrated Management Information System
TIN	Taxpayer Identification Number
TRDB	Tax Return Data Base
TSA	Terminal Security Administrator
TSID	Terminal Security Identification
TVR	Terminal Vector Record
UCCP	Unit Command Code Profile
UNAX	Unauthorized Access
USGCB	United States Government Configuration Baseline
USR	Unit Security Representative

Exhibit 10.8.34-2 (Cont. 2) (11-21-2022)**Terms and Acronyms**

UWR	Unified Work Request
W&I	Wage and Investment

Exhibit 10.8.34-3 (11-21-2022)**Related Resources**

Other handbooks and Internal Revenue Manuals contain information relating to IDRS or security that may be helpful to IDRS security personnel. These include the following:

• IRM 3.12.32, <i>Error Resolution - General Unpostables</i>
• IRM 6.751.1, <i>Discipline and Disciplinary Actions: Policies, Responsibilities, Authorities, and Guidance</i>
• IRM 10.5.5, <i>Privacy and Information Protection - IRS Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements</i>
• IRM 10.5.7, <i>Privacy and Information Protection, Use of Pseudonyms by IRS Employees</i>
• IRM 10.5.8, <i>Privacy and Information Protection, Sensitive But Unclassified (SBU) Data Policy: Protection SBU in Non-Production Environments</i>
• IRM 10.8.1, <i>Information Technology (IT) - Security Policy and Guidance</i>
• IRM 10.8.2, <i>Information Technology (IT) Security- IT Security Roles and Responsibilities</i>
• Document 12926-SA, <i>SACS Security Accounts Administrator Command Code Procedures</i>
• Document 12926-USR, <i>SACS Unit Security Representative Command Code Procedures</i>
• Document 12990, Record Control Schedule (RCS)
• NIST SP 800-53 Rev 5, <i>Security and Privacy Controls for Federal Information Systems and Organizations</i> , December 10, 2020
• TD P 85-01 Version 3.1.3, <i>Treasury Information Technology Security Program</i> , February 28, 2022

Exhibit 10.8.34-4 (11-21-2022)
Distribution Procedures

#

#

[illegible]

#

##

#

--	--	--	--

#

#####

[illegible]

[illegible][illegible]

#

[illegible][illegible]

#####

[illegible]

Exhibit 10.8.34-12 (11-21-2022)**IDRS Office Identifiers, Organization Code Ranges, and Unpostable Holding Units**

This exhibit defines the series of organization codes, IDRS Office Identifiers (OI), and Unpostable Holding Units for use by IRS Business Divisions.

#

Exhibit 10.8.34-13 (11-21-2022)**IDRS Organization Codes — IRS Campuses**

This exhibit defines the series of organization codes for use by the IRS campuses. These offices have Office Identifiers (OI) from 01 to 10.

#

Exhibit 10.8.34-14 (11-21-2022)**IDRS Organization Codes - Wage and Investment (W&I) Area Offices**

This exhibit defines the series of organization codes for use by the Wage and Investment Area offices. These offices have Office Identifiers (OI) from 11 to 17.

#

Exhibit 10.8.34-15 (11-21-2022)**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 Area offices. These offices have Office Identifiers (OI) from 21 to 27 and 35 except for SB/SE Communication, Liaison & Disclosure organization user accounts will remain in OI 79.

#

Exhibit 10.8.34-16 (11-21-2022)**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 Office Identifiers (OI) as follows: Appeal (66), SBSE - Disclosure (79), Communication and Liaison (79), Counsel (69), Criminal Investigation (60), Large and Midsize Business (50), Tax Exempt and Government Entities (40), and Taxpayer Advocate (63).

#

Exhibit 10.8.34-17 (11-21-2022)**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.

This exhibit is available on the IDRS Security website: <https://portal.ds.irsnet.gov/sites/CyberAI/ITSI/IDRSSecurity/SitePages/Home.aspx>

#

Exhibit 10.8.34-18 (11-21-2022)**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]

[illegible]

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

#

[illegible][illegible]

#####

[illegible]

[illegible]

#####

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

#

#

#

