



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

9.12.1

FEBRUARY 13, 2024

## EFFECTIVE DATE

(02-13-2024)

## PURPOSE

- (1) This transmits revised IRM 9.12.1, Miscellaneous Administrative Procedures.

## MATERIAL CHANGES

- (1) IRM 9.12.1.1 Added: Purpose, Audience, Policy Owner, Program owner and Primary Stakeholder, in bullet format under Program Scope and Objective to meet Internal Control requirements.
- (2) IRM 9.12.1.1.1 Added Background subsection to meet Internal Control requirements.
- (3) IRM 9.12.1.3 Updated verbiage in second sentence from; on a database, to read; in the official tax return inventory database maintained by CI.
- (4) IRM 9.12.1.7.4 Relocated Access to the Criminal Investigation Network by Criminal Investigation Employees, Task Force Officers and Contractors from IRM subsection from 9.11.4.19 to 9.12.1.7.4
- (5) IRM 9.12.1.7.4(3) Added instructional verbiage to 9.12.1.7.4 (3)The test must check for the drugs specified by the *IRS Drug Free Work Program* and be dated no earlier than 30 days prior to the request for CI system network and applications access.
- (6) IRM 9.12.1.7.5 Relocated Access to the Criminal Investigation Network by Non-Criminal Investigation Personnel from IRM subsection from 9.11.4.19.1 to 9.12.1.7.5
- (7) IRM 9.12.1 Updated his/her to their throughout

## EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 9.12.1 dated November 16, 2022.

## AUDIENCE

CI

Guy Ficco, for James Lee, Chief, Criminal Investigation



9.12.1

Miscellaneous Administrative Procedures

## Table of Contents

9.12.1.1 Program Scope and Objective

9.12.1.1.1 Background

9.12.1.1.2 Authority

9.12.1.1.2.1 Acronyms

9.12.1.2 Daily Record of Activity Diary

9.12.1.3 Mandatory Guidelines for Tax Return Inventory Control

9.12.1.4 Security of Communications

9.12.1.4.1 Use of Double Sealed Mailing Envelopes

9.12.1.4.2 Discussion of Official Business

9.12.1.4.3 Use of Words “Top Secret,” “Secret ” and “Confidential”

9.12.1.4.4 Transmitting Documents by Mail

9.12.1.4.5 Facsimile Transmission of Tax Information

9.12.1.4.6 Electronic Mail

9.12.1.5 Recognition Programs

9.12.1.5.1 Criminal Investigation Chief’s Award

9.12.1.6 Confidential Financial Disclosure Program for CI Employees

9.12.1.7 Criminal Investigation Activities Within a Disaster Area

9.12.1.7.1 Coordination with U. S. Attorney’s Office

9.12.1.7.2 Initiation of Investigation

9.12.1.7.3 Assistance to Local Law Enforcement

9.12.1.7.4 Access to the Criminal Investigation Network by Criminal Investigation Employees, Task Force Officers and Contractors

9.12.1.7.5 Access to the Criminal Investigation Network by Non-Criminal Investigation Personnel



9.12.1.1  
(02-13-2024)  
**Program Scope and  
Objective**

- (1) This section contains administrative procedures with respect to miscellaneous topics.
- Purpose- To provide guidance to CI employees
  - Audience - All of CI
  - Policy Owner - All of CI
  - Program Owner - All of CI
  - Primary stakeholders - All of CI

9.12.1.1.1  
(02-13-2024)  
**Background**

- (1) The IRS Restructuring and Reform Act of 1998 resulted in a complete restructuring and reformatting of the IRM to align with IRS business processes. One of the primary goals of IRS modernization was to restore and maintain the IRM as the single, official compilation of IRS policies, procedures, and guidelines. The IRM is the primary source of instructions to staff.

9.12.1.1.2  
(11-16-2022)  
**Authority**

- (1) See IRM 9.1.2, for the delegated authority relating to 9.12.1 Miscellaneous Administrative Procedures.

9.12.1.1.2.1  
(11-16-2022)  
**Acronyms**

- (1) Acronym table lists commonly used acronyms and their definitions

Acronym	Definition
ASAC	Assistant Special Agent in Charge
CI	Criminal Investigation
CSA	Compliance Support Assistant
DEO	Deputy Ethics Official
DLN	Document Locator Number
E-Mail	Electronic Mail
FOUO	For Official Use Only
HCO	Human Capital Office
HQ	Headquarters
IDRS	Integrated Data Retrieval System
LEAP	Law Enforcement Availability Pay
LEM	Law Enforcement Manual
LOU	Limited Official Use
OGE	Office of Government Ethics
QRP	Questionable Refund Program
RPP	Return Preparer Program
SAC	Special Agent in Charge
SBU	Sensitive But Unclassified

Acronym	Definition
SDAC	State Disaster Assistance Coordinator
SIA	Supervisory Investigative Analyst
SM	Secure Messaging
SSA	Supervisory Special Agents
TFIA	Tax Fraud Investigative Assistants

## 9.12.1.2

(11-16-2022)

**Daily Record of Activity  
Diary**

- (1) All technical and investigative support Criminal Investigation (CI) personnel, (except Supervisory Special Agents (SSA), Supervisory Investigative Analysts (SIA) and higher management officials), and investigative support personnel are required to maintain a daily record of activities in an electronic data file (CI Diary). Non-technical personnel at the field office, area office, and Headquarters (HQ) levels not directly involved in investigative activities are not required to maintain a daily record of activities. Such non-technical personnel include: budget analysts, program analysts, management analysts, etc.
- (2) The following instructions apply to the CI Diary:
  - a. Keep diaries current and up-to-date.
  - b. Entries should be brief but detailed enough to describe the employee's activities with respect to official matters, such as investigative actions, leave, Law Enforcement Availability Pay (LEAP), overtime/credit/compensatory hours worked, travel expenses, vehicle log including home-to-work entries, official expenditures, etc.
  - c. Entries should cover important activities, such as initial interview of taxpayers, interviews of return preparers or key witnesses.
  - d. Entries should be of sufficient length to describe the event. This would include sources, dates of origin, and other facts and circumstances involved in obtaining leads and evidence in investigations.
  - e. Law Enforcement Availability Pay (LEAP) entries should be specific as to the time and details of all activities.
- (3) Diaries will be inspected by management officials to ensure that instructions pertaining to diary maintenance are being observed. Annually as directed, special agents, investigative analysts, tax fraud investigative assistants (TFIA) and compliance support assistants (CSA) will transfer a copy of their CI Diary data file to their immediate manager for review. The manager will access the Manager Review feature of the CI Diary and review the diary data file of their subordinate personnel. This review must be completed as soon as practicable, since subordinate personnel cannot make entries in their CI Diary until the reviewed data file is e-mailed back by the manager and saved to the CI Diary data file by the employee.
- (4) All diaries or calendars used to maintain a daily record of activities should be retained by the CI head of office to which the employee is assigned. In the event an employee transfers within CI, the head of office will forward the employee's diaries or calendars to the head of office to which the employee is transferred. Diaries or calendars of an employee will be made available to the former field office upon request.

9.12.1.3  
(11-16-2022)  
**Mandatory Guidelines  
for Tax Return Inventory  
Control**

- (1) A separate record of all original tax returns in the custody of field office personnel will be maintained by the Special Agent in Charge (SAC). These original documents include Questionable Refund Program (QRP) and Return Preparer Program (RPP) documents that contain a Document Locator Number (DLN).

**Note:** At the option of the Director, Field Operations, the SAC may delegate this responsibility to an SSA/SIA.

- (2) These procedures require appropriate security for original tax returns and documents containing DLNs to prevent unauthorized disclosures. These original documents should not be retained by CI longer than necessary.
- (3) The SAC or SSA/SIA (if delegated this responsibility) will designate a member of their professional staff as the designee to be responsible for the request, receipt, control and custody of the inventory of tax returns.
- (4) To request tax returns or documents containing a DLN, requestors will submit a complete and correct request through the established investigative support request system. SIA assignment of the request to the designee, serves as management approval. The designee will input the request through the Integrated Data Retrieval System (IDRS) and maintain the request documentation in an authorized server location.
  - a. A special agent assigned to assist government attorneys will not request tax returns or tax return information in response to ex parte orders. The Disclosure Officer serving the field office will request all returns and return information in response to an ex parte order. To facilitate expeditious handling, government attorneys should be directed by special agents to forward ex parte orders directly to the Disclosure Officer.
  - b. The provisions of 26 USC §6103 do not authorize CI to secure returns or return information in response to ex parte orders. Failure to adhere to these provisions could result in an unauthorized disclosure (see IRM 11.3, Disclosure of Official Information, and Delegation Order 11-2, Authority to Permit Disclosure of Tax Information and to Permit Testimony or the Production of Documents).
- (5) All original returns, documents bearing DLNs and transmittals; Document Charge Out (Form 4251); and Document Transmittal (Form 3210) should go directly to the designee. The designee will maintain document request, receipt, custody, and assignment information in the official tax return inventory database maintained by CI, and notify the requestor when documents are received.
- (6) The designee as the primary custodian will exercise exclusive control of the database described in the preceding paragraph and will have custody of all original tax returns and documents with DLNs. The delegate, as back-up, will have access to only the database information described in the preceding paragraph. The primary designee will keep the original tax returns and any related documents in a locked cabinet. The designee will also use Form 3210 as a controlling document or logbook to acknowledge transfer or receipt of original returns when they are assigned to special agents. Special agents will work from a copy of an original return and will not normally be assigned or retain the original for extended periods. Original tax return(s) should only be assigned to a special agent when needed for signature verification of the taxpayer and return preparer for grand jury or trial proceedings.

## 9.12 Administrative and Recordkeeping Matters

- a. A certified copy of the original tax return will be introduced as the grand jury or trial exhibit. The original tax return will remain in the custody of IRS.
- (7) Special agents will periodically provide the designee with a list of all tax returns that are no longer needed for retention in the field office. At a minimum, the returns assigned to a special agent will be reviewed annually during their workload review to determine if the returns are still needed.
- (8) Periodically, the designee will recharge original tax returns to files and update the tax returns status on the database.
- (9) By November 30th of each year, the designee will perform database verifications to ensure that returns requested have been received or recharged to files, and that both database and related assignment documents match.
  - a. There shall be a 100% physical verification of every original tax return in the custody and control of the designee.
  - b. The SSA/SIA shall assign someone other than the designee to perform the 100% verification to ensure a separation of duties. If possible, the person performing the verification shall be a designee from another group within the field office.
  - c. The SSA/SIA shall be provided with the database verification by December 15th of each year so that he/she can take necessary actions to correct any discrepancies and ensure the effectiveness of the operation. The SSA/SIA will initial and date the database verification and retain it for two years. The retained verifications will show the actions taken to correct any discrepancies.
- (10) By December 15th of each year, the SSA will sample Forms 4844, Request for Terminal Action, to ensure the designee inputs only approved requests for any tax return.
- (11) As part of their operational review, the SAC or Assistant Special Agent in Charge (ASAC) will verify the accuracy of the original tax return inventory and the SSA's original tax return assignments to the special agents. In instances where tax returns were secured as a result of a related statute determination (see IRM 9.3.1, Disclosure), the SAC or ASAC will ensure that a copy of the related statute determination memorandum is attached to the tax return or retained in the related tax return inventory file.

### 9.12.1.4 (03-01-2005) Security of Communications

- (1) All communication must be protected from unauthorized disclosure. This includes oral, written and electronic communication.

### 9.12.1.4.1 (01-28-2004) Use of Double Sealed Mailing Envelopes

- (1) Written communications involving matters to which access is limited should be mailed in double sealed envelopes marked, "to be opened by addressee only." This applies to:
  - a. Investigative, statistical and management reports
  - b. Collateral requests and replies
  - c. Memoranda of any kind

**Note:** When there is doubt as to whether or not double sealed mailing should be used, it should be resolved in favor of using double sealed mailing.



9.12.1.4.2  
(12-16-2008)

**Discussion of Official  
Business**

- (1) Official matters should not be discussed in public or within the hearing of the public (see IRM 9.3.1).

9.12.1.4.3  
(07-01-2011)

**Use of Words "Top  
Secret," "Secret " and  
"Confidential"**

- (1) The designations "Top Secret", "Secret", and "Confidential" may be used only on documents containing information affecting the national security of the United States as defined in Executive Order 12958, Classified National Security Information as amended.
- (2) Sensitive But Unclassified (SBU) shall be the primary term used to mark sensitive but unclassified information originating within Treasury/Bureau offices. Previous designations to label sensitive information like Limited Official Use (LOU), For Official Use Only (FOUO), Eyes Only, etc. shall be discontinued in identifying SBU information produced within Treasury/Bureaus unless a particular term is authorized by law, statute or agency regulation or as identified by the Freedom of Information Act (FOIA) or the Privacy Act. Except for the term "Law Enforcement Sensitive" used by Criminal Investigation (CI), no other terms shall be applied to Treasury/Bureau originated sensitive information determined to be SBU unless authorized by law, statute, or regulation.
- (3) Any documents that retain the designation "LOU", "FOUO", "OUO", etc. should be considered as designated SBU/Law Enforcement Sensitive.

**Note:** Unauthorized disclosure of SBU may reduce the effectiveness of tax administration, violate law, adversely affects the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act or other laws. The Law Enforcement Manual (LEM) Documents Part 9 are "Law Enforcement Sensitive" and requires special handling to prevent its loss, misuse, alteration or unauthorized disclosure (see IRM 11.3.12, Designation of Documents).

9.12.1.4.4  
(07-15-2002)

**Transmitting Documents  
by Mail**

- (1) When transmitting documents by regular mail, registered mail, certified mail or other express service, confirmation of delivery will be used if any of the following documents are included in the transmittal:
  - a. Administrative file, including original tax returns
  - b. Special agent's report (SAR)
  - c. Exhibits to SAR
  - d. Supplemental report
- (2) Should confirmation of delivery not be received by the office transmitting such files or documents within a reasonable period, not to exceed 15 days, inquiry is to be made through the regular channels of the delivery service in regard to the apparent failure of registered mail or express service to reach the addressee.
  - a. Information concerning the delayed or lost transmittals should be forwarded to the addressee.
  - b. Steps should be taken as appropriate or necessary to duplicate the contents of the original transmittal to permit the addressee to proceed with the proposed necessary action.

9.12.1.4.5  
(12-16-2008)  
**Facsimile Transmission of Tax Information**

(1) The legal restrictions for facsimile transmission of tax information is the same as for responding to an inquiry for tax information by telephone or mailing tax information to third parties. Guidelines regarding the faxing of return and return information can be found in IRM 11.3.1, Introduction to Disclosure.

9.12.1.4.6  
(12-16-2008)  
**Electronic Mail**

(1) Employees may not use e-mail to transmit SBU data unless they use the IRS Secure Messaging (SM) system. Secure Messaging allows users to encrypt e-mail messages and attachments for transmission between IRS employees. However, both the sender and recipient must have SM to protect the e-mail.

(2) See IRM 11.3.1 (subsection 11.3.1.14.2, Electronic Mail and Secure Messaging, and IRM 10.8.1, Policy and Guidance (subsection 10.8.1.4.6.3, Electronic Mail (E-Mail) Security) for additional information regarding e-mail guidelines.

9.12.1.5  
(07-01-2011)  
**Recognition Programs**

(1) There are various CI and IRS employee recognition programs. Procedures for preparing and processing award recommendations can be found on CI Connections on the Human Resources Web page; Finance Web page; and the IRWeb site on the IRS Human Capital Office (HCO) Web page.

9.12.1.5.1  
(12-16-2008)  
**Criminal Investigation Chief's Award**

(1) The Criminal Investigation Chief's Award may be presented to individuals who have made a significant contribution benefiting CI nationwide. Those who may qualify for this award are both internal and external. CI and IRS employees, as well as law enforcement or regulatory officials, state attorneys, Department of Justice Attorneys, Assistant United States Attorneys and United States Attorneys whose contribution was national in scope will be considered.

(2) The Chief's award can be granted when the Services, or other personal efforts performed by an individual official or an organization, have substantially exceeded normal standards and expectations and have a national impact on the CI mission.

(3) Submit the request in writing, to the respective Director, Field Operations or the Headquarters Directors' for Operations, Policy and Support; Strategy; Refund Crimes; or Technology Operations and Investigative Services for approval. This request should be submitted at least 60 days prior to the date needed to ensure sufficient time to order the award and engraving.

(4) Written request for the Chief's award must contain the following information:

- Name of the recipient
- Recipient's position or title
- Narrative description of the individual's or organization's contribution and how they contributed to the nationwide accomplishment and success of CI's mission
- Projected presentation date i.e., when and where the award will be presented

(5) After approval by the Director, Field Operations, or HQ Director, the request will be forwarded to the Director, Communications & Education to coordinate final approval by the Chief, CI.

(6) If approved by the Chief, CI the respective Director, Field Operations or HQ Director will be responsible for planning the award presentation at a time con-

venient for both the Chief, CI and the recipient. This will be coordinated with the Director, Communications & Education.

- (7) Should a request for this award be disapproved, a local field office award may be given subject to the approval of the SAC.

9.12.1.6  
(03-01-2005)  
**Confidential Financial  
Disclosure Program for  
CI Employees**

- (1) In order to avoid conflicts of interest, certain executive branch employees must file a Confidential Financial Disclosure Report upon entering covered positions and yearly thereafter with the Office of Government Ethics (OGE).
- (2) Confidential financial disclosure is subject to a number of legal requirements. The filing of Confidential Financial Disclosure Reports is addressed in the Ethics in Government Act of 1978 (as amended); Title 5 of the Code of Federal Regulations, Part 2634, Subpart I; and Treasury Directive 61-02. In-depth information on the Service's Confidential Financial Disclosure Reporting Program can be found on the Service-wide Ethics Program Web site. The Desk Procedures for Administering the IRS' Confidential Financial Disclosure Program in CI can be found on the CI Human Resources Web page.
- (3) The Associate Chief Counsel (General Legal Services) is the Deputy Ethics Official (DEO) for the IRS. The DEO provides advice to IRS employees concerning the OGE Standards of Ethical Conduct, the Treasury Supplemental Standards, the Treasury Rules of Conduct, conflicts of interest, and related statutes and regulations.

9.12.1.7  
(11-16-2022)  
**Criminal Investigation  
Activities Within a  
Disaster Area**

- (1) The SAC may consult with the State Disaster Assistance Coordinator (SDAC) to consider the appropriateness of limiting enforcement activities until the conditions of the disaster have been alleviated. The SAC may issue guidelines covering general types of proscribed activities, or may choose to require pre-approval at the SSA level for various activities on a case-by-case basis.

9.12.1.7.1  
(07-29-2013)  
**Coordination with U. S.  
Attorney's Office**

- (1) In grand jury investigations and investigations pending legal action, any decisions to limit or suspend activities must be closely coordinated with the U.S. Attorney's Office.

9.12.1.7.2  
(07-29-2013)  
**Initiation of Investigation**

- (1) Some financial crimes and tax evasion schemes, such as profiteering and price gouging, proliferate during and after disasters. Criminal Investigation may wish to focus attention on these areas as a potential source of investigations.

9.12.1.7.3  
(07-29-2013)  
**Assistance to Local Law  
Enforcement**

- (1) The SAC may wish to consider making special agents available to assist local law enforcement authorities in a disaster. General Legal Services shall be consulted to determine the legal authority and potential liability issues involved before any such assistance is provided.

9.12.1.7.4  
(03-17-2021)  
**Access to the Criminal  
Investigation Network by  
Criminal Investigation  
Employees, Task Force  
Officers and Contractors**

- (1) The successful completion of a pre-employment background investigation is required for CI employees to access the CI system network and applications.
- (2) The completion and approval of the TFO application, Memorandum of Understanding, and CI TFO Mandatory Briefings Certification is required for CI TFOs to access the CI system network and applications.

## 9.12 Administrative and Recordkeeping Matters

- (3) Contracts for individuals requiring CI network access will include a requirement that the contracting company provide results showing the individual assigned to a CI contract has passed a drug test and preliminary background investigation prior to access being granted to the CI system network and applications. The test must check for the drugs specified by the *IRS Drug Free Work Program* and be dated no earlier than 30 days prior to the request for CI system network and applications access.
- (4) All CI employees, TFOs, and contractors will be granted access to the CI network and appropriate applications following a request by the first-line manager. In making a request for access the CI network, the manager will:
  - a. Utilize the current network and application request system to add the employee/TFO/contractor to their application system workgroup.
  - b. Initiate the action to request CI network access for the employee/TFO/contractor. When approved, the Technology Operations and Investigative Services section will issue a login and password.
  - c. Ensure the employee/TFO/contractor reads and acknowledges the online Information Systems Security Rules and completes the mandatory Computer Security briefing.

9.12.1.7.5  
(10-06-2020)

### Access to the Criminal Investigation Network by Non-Criminal Investigation Personnel

- (1) In instances where there is a bona fide business need for non-CI personnel to access the CI network, a request for CI system access and CI hardware will be made by the SAC or appropriate management official to their Executive Director.
- (2) A template for the access request is available through the CI Unified Checklist or current document management system. The request must include:
  - a. The non-CI personnel name, current agency, and position. (If the individual is a contractor for another agency, the name of the agency responsible for the contract)
  - b. Justification for the individual requiring CI system access;
  - c. The timeframe for which access is being requested (limited to one year, but extension can be requested as noted in below);
  - d. Confirmation that the non-CI personnel is a US Citizen (See IRM Section 10.23.2.3 - Citizenship Requirements); and
  - e. The steps taken to verify a background investigation was completed by the employing agency.

**Note:** Executive Order 12968, Section 2.4, Reciprocal Acceptance of Access Eligibility Determination, allow background investigations and eligibility determinations for classified information access to be mutually and reciprocally accepted by all agencies. All Federal employees are presumed to have a background investigation that meets this requirement.

- (3) The Executive Director will either approve or disapprove the access request.
- (4) The Executive Director will forward the approved access request to the Executive Director of Technology Operations and Investigative Services for review to ensure consistency throughout CI. The SAC or management official will ensure non-CI personnel complete the System Access Computer Security briefing. The establishment of an account will be made through the Director, Technology Operations and Investigative Services or their designee.

- (5) The account will remain active until:
  - a. Completion of the approved access period;
  - b. Removal from the network before the end of the access period (no longer needed); or
  - c. Removal from the network to meet the needs of IRS.
- (6) An extension of the access period can be requested by the originating SAC or management official and approved by the Executive Director by e-mail. The approved extension will be forwarded to the Executive Director, Technology Operations and Investigative Services.
- (7) Non-CI personnel granted access to the CI network will be allowed access only through CI imaged hardware. Connectivity to the CI network will not be allowed through use of another IRS business unit, agency, or contractor computer.

