MANUAL TRANSMITTAL

9.4.7

Department of the Treasury
Internal Revenue Service

JULY 5, 2024

EFFECTIVE DATE

(07-05-2024)

PURPOSE

(1) This transmits revised text for IRM 9.4.7, Consensual Monitoring.

MATERIAL CHANGES

(1) Added required Internal Controls to comply with IRM 1.11.2.2.4, Address Management and Internal Controls and IRM 1.4.2, Resource Guide for Managers Monitoring and Improving Internal Controls.

(2) Subsection 9.4.7.3.1(a) updated verbiage to current procedures.

(3) Subsection 9.4.7.3.2 removed “these situations” and added “circumstance described in paragraph 1(c) above”.

(4) Added subsection 9.4.7.3.7 “When requesting an undercover operation in CIMIS, a consensual monitoring is requested simultaneously.”

(5) Subsection 9.4.7.4.1(1) removed first sentence and added verbiage for current procedures.

(6) Added subsection 9.4.7.4.3(3)(b) “IRS personnel are conducting the interview.”

(7) Subsection 9.4.7.7 updated verbiage to current procedures.

(8) Subsection 9.4.7.8(1) updated director title to “Director, Special Investigative Techniques” and removed “induction coils”.

(9) Subsection 9.4.7.8(3) removed “induction coils”.

(10) Subsection 9.4.7.8(4) removed “induction coils”.

(11) Subsection 9.4.7.8(5) updated verbiage to current procedures.

(12) Subsection 9.4.7.8(7) removed “this” and “induction coils”.

(13) Additional revisions, deletions, and grammatical changes were made throughout the section, that did not result in substantive changes but contributed to procedural clarity of the subject matter.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 9.4.7, Consensual Monitoring dated September 13, 2013.

AUDIENCE

Criminal Investigation

Shea C. Jones
Acting Deputy Chief, Criminal Investigation
for
Guy A. Ficco
Chief, Criminal Investigation

9.4.7
CONSENSUAL MONITORING

Table of Contents

9.4.7.1
(07-05-2024)
Program Scope and Objectives

(1) Purpose: This section contains policy and procedural information concerning the investigative use of electronic or mechanical monitoring devices with the consent of one or more parties to conversations. For procedural reasons, conversations are categorized as either telephonic or non-telephonic.

Note: Before any monitoring may take place, there must be no question as to whether the use of any investigative device is legal under the circumstances.

(2) Audience: All Criminal Investigation (CI) employees.

(3) Policy Owner: Director, Special Investigative Techniques (SIT).

(4) Program Owner: Director, Special Investigative Techniques (SIT).

(5) Primary Stakeholders: All CI employees.

(6) Contact Information: To make changes to this IRM section email CIHQIRM@ci.irs.gov.

9.4.7.1.1
(07-05-2024)
Background

(1) Special Investigative Technique has oversight responsibilities for the authorization and conduct of undercover operations, witness protection, electronic surveillance, and use of informants. SIT provides first class support of operations and to provide innovative covert techniques that CI's mission while upholding integrity, safety, and accountability.

9.4.7.1.2
(07-05-2024)
Authority

(1) See IRM 9.1.2, Authority for the delegated authority relating to IRM 9.4.7, Consensual Monitoring.

9.4.7.1.3
(07-05-2024)
Roles and Responsibilities

(1) The Director, Special Investigative Techniques is responsible for developing, maintaining, and overseeing this IRM and ensuring compliance with current policies and procedures.

9.4.7.1.4
(07-05-2024)
Program Management and Review

(1) The Director, Special Investigative Techniques will:

a. Review the IRM annually,
b. Update the IRM when content is no longer accurate and reliable to ensure employees correctly complete their work assignments,
c. Incorporate all permanent interim content into the next version of the IRM section prior to the expiration date.

9.4.7.1.5
(07-05-2024)
Program Controls

(1) The Director, Special Investigative Techniques will review the instructions and guidelines relating to all IRS documents for procedural, operational, and editorial changes.

9.4.7.1.6
(07-05-2024)
Acronyms

(1) The table lists commonly used acronyms and their definitions:

Acronym	Definition
BOP	Bureau of Prisons
CI	Criminal Investigation

CIMIS	Criminal Investigation Management Information System
DOJ	Department of Justice
SAC	Special Agent in Charge
SIT	Special Investigative Techniques
USMS	United States Marshals Service

9.4.7.1.7
(07-05-2024)
Related Resources

(1) IRM 9.4.2, Sources of Information.

(2) IRM 9.11.3, Investigative Property.

9.4.7.2
(09-13-2013)
Consensual Monitoring Defined and Distinguished

(1) The term consensual monitoring, as used herein, means the investigative interception, overhearing, or recording of a private conversation by the use of mechanical, electronic, or other devices with the consent of at least one, but not all, of the participants (as contrasted to non-consensual monitoring, where no participant consents). Consensual monitoring may be used in primary and subject investigations. Telephonic consensual monitoring may be used in general investigations.

(2) Supervisory approval is not required for monitoring conversations with the consent of **all** parties to the conversation.

(3) The monitoring of conversations with the consent of one of the participants may be used whenever it is both appropriate and necessary to gather evidence related to a criminal offense. However, this technique is subject to careful oversight in order to avoid any unwarranted invasion of privacy or perception of impropriety.

(4) To protect the integrity of all consensual monitoring activities:

a. Recordings must be preserved in their entirety, including information unrelated to the investigation.
b. A record of all contacts with the subject of the monitoring request must be maintained. The record must reflect all contacts with the subject, including those that were not recorded. This record will include the consensual monitoring authorization number, the investigation number, the date of contact, and the subject of that contact. An explanation as to why a contact was not monitored must also be included.

(5) The Criminal Investigation Management Information System (CIMIS) Special Investigative Techniques (SIT) activity area will be used to request all consensual monitoring. Special agents may make modifications to original consensual monitoring requests in CIMIS using the Request Consensual Monitoring Modification activity in CIMIS. Modification types include extensions of time, closings, corrections to the original request, and other modifications.

9.4.7.3
(09-13-2013)
Consensual Monitoring of Telephonic Conversations

(1) This section contains policies and procedures concerning consensual monitoring of telephonic conversations.

9.4.7.3.1
(07-05-2024)
Authorization of Telephonic Consensual Monitoring

(1) Generally, the Special Agent in Charge (SAC) has authority to approve telephonic consensual monitoring requests. However, in the following situations, additional authorization is required:

a. All consensual monitoring requests require some level of approval. If the consensual monitoring request relates to an undercover operation, consult an Undercover Program Manager (UPM) to determine what level of approval is required.

b. The authorization of the Chief or Deputy Chief, Criminal Investigation (CI), is required for consensual monitoring of telephonic conversations where the recording device is to be installed in a place or manner that will create the risk of inadvertent prohibited non-consensual monitoring. The request for approval must contain sufficient information to apprise the authorizing officials of the need for installing the recording device in the manner proposed and the precautions that will be taken to prevent non-consensual monitoring.

c. The approval of the Director, Operations Policy and Support, and the Director, Office of Enforcement Operations, Criminal Division, Department of Justice (DOJ), is required for monitoring telephonic conversations when:

- The monitoring relates to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years.
- The monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his/her official duties.
- Any party to the communication is a member of the diplomatic corps of a foreign country.
- Any party to the communication is/has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
- The consenting or non-consenting person is in the custody of the Bureau of Prisons (BOP) or the United States Marshals Service (USMS).
- The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the field office where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

(2) The CIMIS SIT activity area will be used to request authorization to use electronic equipment and consensual monitoring. All details of the consensual monitoring will be entered into CIMIS and linked to an existing, open, approved investigation. Special agents may also request modifications to the consensual monitoring using the Request Consensual Monitoring Modification Activity.

Modification types include extensions of time, closings, corrections to the initial request, and changes to the linked investigation. Expiration of a consensual monitoring authorization associated with a Group I or II undercover operation will coincide with the expiration of the undercover authorization period, unless the monitoring involves a circumstance described in paragraph 1(c) above. Monitoring authorizations associated with a circumstance described in paragraph 1(c) above are limited to 90 days but may be renewed upon submission of a written request to the DOJ, Office of Enforcement Operations.

a. When the recording device will be concealed, the request must include an explanation of the precautions taken to ensure that non-consensual monitoring will not occur. For example, the monitoring device will be removed or disconnected after each authorized recording; or the monitoring device and telephone will be in a secure area with access limited to those individuals involved in the monitoring.
b. IRM 9.11.3, Investigative Property, contains information on the types of equipment that can be used and specific restrictions and responsibilities regarding the use of sensitive-type investigative equipment.

(3) The officials approving the monitoring requests must be added to the grand jury access list for all grand jury investigations.

(4) A Confidential Informant or Cooperating Witness consenting to the monitoring of a conversation must be established as such pursuant to IRM 9.4.2, Sources of Information.

(5) At the discretion of the approving official, the request may be oral, provided authorization to use electronic equipment and consensual monitoring is requested in the CIMIS SIT activity area within 5 working days.

(6) A Form 6795, Consensual Monitoring Report, will be submitted to the approving authority within 15 working days after the conclusion of monitoring activities (or attempted monitoring activities) for each specific authorization. The Form 6795 must include a list of all monitoring that took place during the monitoring period. The completed Forms 6795 must be submitted electronically to Special Investigative Techniques. If no monitoring occurred, the report is due within 15 working days of the authorization's expiration date. All consensual monitoring requests related to undercover operations are requested in CIMIS simultaneous to requesting the undercover operation in CIMIS.

(7) When requesting an undercover operation in CIMIS, a consensual monitoring is requested simultaneously.

9.4.7.4 (09-13-2013) Consensual Monitoring of Non-Telephonic Conversations

(1) This section contains policies and procedures concerning consensual monitoring of non-telephonic conversations.

9.4.7.4.1 (07-05-2024) Authorization for Non-Telephonic Consensual Monitoring

(1) All consensual monitoring requests require some level of approval. If the consensual monitoring request relates to an undercover operation, consult an Undercover Program Manager (UPM) to determine what level of approval is required. The Director, Field Operations is the approving official in non-telephonic consensual monitoring not related to an undercover operation and when the circumstances described in paragraphs (2) or (3) are not present.

(2) The authorization of the Chief or Deputy Chief, CI, is required for consensual monitoring of non-telephonic conversations where the recording device is to be installed in a place or manner that will create the risk of an inadvertent prohibited non-consensual monitoring. The request for approval must contain sufficient information to apprise the authorizing officials of the need for installing the recording device in the manner proposed and the precautions that will be taken to prevent non-consensual monitoring.

(3) The approval of the Director, Global Operations Policy and Support, and the Director, Office of Enforcement Operations, Criminal Division, DOJ, is required for monitoring non-telephonic conversations when:

a. The monitoring relates to an investigation of a member of Congress, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years.
b. The monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his/her official duties.
c. Any party to the communication is a member of the diplomatic corps of a foreign country.
d. Any party to the communication is/has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.
e. The consenting or non-consenting person is in the custody of the BOP/USMS.
f. The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the field office where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

(4) The CIMIS SIT activity area will be used to request authorization to use electronic equipment and consensual monitoring. All details of the consensual monitoring will be entered into CIMIS and linked to an existing, open, approved investigation.

(5) Special agents may request modifications to the consensual monitoring using the Request Consensual Monitoring Modification Activity in CIMIS. Modification types include extensions of time, closings, corrections to the initial request, and changes to the linked investigation.

(6) Expiration of a consensual monitoring authorization associated with a Group I or II undercover operation will coincide with the expiration of the undercover authorization period, unless the monitoring involves a circumstance described in paragraph 3 above. Monitoring authorizations associated with these situations are limited to 90 days but may be renewed upon submission of a written request to the Department of Justice, Office of Enforcement Operations.

a. When the recording device will be concealed, the request must include an explanation of the precautions taken to ensure that non-consensual monitoring will not occur. For example, the monitoring device will be removed or disconnected after each authorized recording; or the monitor-

ing device and telephone will be in a secure area with access limited to those individuals involved in the monitoring.

b. IRM 9.11.3, Investigative Property, contains information on the types of equipment that can be used and specific restrictions and responsibilities regarding the use of sensitive-type investigative equipment.

(7) Consensual monitoring approving officials must be included on the grand jury access list for all grand jury investigations

(8) A Confidential Informant or Cooperating Witness consenting to the monitoring of a conversation must be established as such pursuant to IRM 9.4.2, Sources of Information.

(9) A Department of Justice (DOJ) Attorney must be consulted concerning the proposed non-telephonic consensual monitoring. The DOJ Attorney's name and position must be entered in CIMIS at the time the request to conduct consensual monitoring is completed.

(10) The CIMIS will assign a consensual monitoring control number.

(11) Form 6795 will be submitted to the approving authority within 15 working days after the completion of the monitoring activities (or attempted monitoring activities) for each specific authorization. The Form 6795 must include a list of all monitoring that took place during the monitoring period. The completed Forms 6795 must be submitted electronically to Special Investigative Techniques. If no monitoring occurred, the report is due within 15 working days of the authorization's expiration date.

9.4.7.4.2
(09-13-2013)
Emergency Authorization for Non-Telephonic Consensual Monitoring

(1) In an emergency, one of the following procedures should be followed:

a. In all situations where the Chief or Deputy Chief, CI, or the Director, Field Operations has approval authority and the emergency needs of an investigation preclude obtaining written advance approval, they may orally authorize consensual monitoring of non-telephonic conversations. As a general rule, when DOJ approval is otherwise required, emergency authorization pursuant to this exception will not be granted where the approving official has in excess of 48 hours to attempt to obtain written advance approval from DOJ.

b. If the Chief or Deputy Chief, CI, grants emergency authorization for situations otherwise requiring written DOJ approval, the Office of Enforcement Operations, DOJ, must be notified within 5 working days. The notification must include an explanation of the emergency and contain all required information under normal circumstances. The authority to grant emergency approval has been delegated by the Commissioner and cannot be re-delegated. Confirmation of emergency approval will be done by memorandum through channels by one of the following: the Chief, CI, or the Deputy Chief, CI.

9.4.7.4.3
(07-05-2024)
Participation with Other Agencies Engaged in Non-Telephonic Consensual Monitoring

(1) Special agents will not participate in the consensual monitoring in a passive or active role unless approval has been obtained for the consensual monitoring by one of the participating agencies.

(2) In situations where another agency has obtained consensual monitoring approval and CI special agents assume an active role, approval is required using the procedures described here in IRM 9.4.7.

(3) The following activities are examples requiring CI approval:

a. IRS personnel are installing or otherwise setting up the recording device(s) and the investigation falls under CI's jurisdiction i.e., the offenses being investigated include money laundering, tax evasion, etc.
b. IRS personnel are conducting the interview.
c. Personnel from the agency that obtained the consensual monitoring authorization are not present at the time of the monitoring.
d. The consenting party is NOT a law enforcement officer. Due diligence must be exercised whenever a relationship is established between an individual consenting to recorded conversations and CI. IRM 9.4.2 defines a cooperating witness and confidential informant. The approval process is also contained in IRM 9.4.2. When giving instruction, direction, and active support in a monitoring situation, CI inherits additional responsibility and risk through the use of the cooperating witness/confidential informant. Authorization for the use of the cooperating witness/confidential informant is required to ensure due diligence on the background and motivation of the consenting party is documented.

(4) In situations where another agency has consensual monitoring approval, special agents do not need written approval from the SAC or Director, Field Operations in the following circumstances:

a. An IRS employee installs or otherwise sets up the monitoring equipment (includes both IRS owned or other equipment) and:

- The investigation is strictly under the jurisdiction of the other agency.
- The offenses do not fall under CI's jurisdiction.
- The monitoring is not conducted at CI's request.
- Local CI management concurs.

b. IRS involvement is limited to providing cover and the consenting party is a law enforcement officer.

9.4.7.5
(09-13-2013)
Extensions

(1) Extensions of additional time for consensual monitoring must be obtained using the Request Consensual Monitoring Modification Activity in CIMIS.

(2) Extension requests must be initiated and approved prior to the date the original authorization expires. Otherwise, the extension request must be considered an original request and Form 6795 is required for the previous authorization.

9.4.7.6
(09-13-2013)
Consensual Monitoring Closing Report(s) Preparation Submission

(1) A Form 6795 will be submitted to Special Investigative Techniques no more than 15 working days after the completion of the monitoring activities (or attempted monitoring activities) for each specific authorization. This report should supplement the information contained in the request for authorization. If no monitoring occurred, the report is due no more than 15 working days from the authorization expiration date.

a. If the consensual monitoring involves a protected witness or a Federal prisoner, a copy of the report will be forwarded by Special Investigative Techniques through the Chief, CI, to the Director, Office of Enforcement Operations, DOJ.

(2) If a monitoring activity occurs without the appropriate approval or occurs outside the period authorized, the SAC will promptly notify, by telephone, the Director, Field Operations of the circumstances involved, who in turn will promptly notify one of the following: the Chief, CI; the Deputy Chief, CI; the Director, Global Operations Policy and Support; or the Director, Special Investigative Techniques. Within 5 workdays the SAC will submit a report through channels to the Chief, CI. This report will set forth all the facts and circumstances surrounding the incident. The Chief, CI, will review the report and take appropriate action.

9.4.7.7
(07-05-2024)
Safeguarding Records of Consensual Monitoring

(1) Whenever technically feasible, the conversations overheard (whether telephonic or non-telephonic) will be recorded by means of a recorder or similar approved device. The original evidence downloaded from the recording device to a storage medium or other permanent record of the conversations and any logs, transcripts, summaries, or memoranda together with copies of all requests for approval and reports shall be specifically safeguarded against improper disclosure. A record of individuals who have had access to this material shall be maintained and retained by the custodian of the evidence.

9.4.7.8
(07-05-2024)
Special Responsibilities for Sensitive Type Investigative Equipment

(1) Except for those devices described in paragraph (3) below, field offices may not purchase, fabricate, or have manufactured any consensual monitoring equipment or accessories without approval from the Director, Special Investigative Techniques, or designee. Additionally, all equipment obtained with approval will be entered into CIMIS by the acquiring office.

(2) Criminal Investigation field offices may maintain an inventory of in-line recording devices, or similar devices for use when consensual telephonic monitoring is approved. These devices may also be used to record conversations where all individuals to the conversation consent.

(3) Field offices may purchase in-line recording devices, or similar devices locally.

(4) Use of personally-owned in-line recording devices, or similar devices is prohibited.

(5) Field Offices will have an inventory with a small number of recorders and technical agents will have available recorders or similar devices. The Field Offices and technical agents will maintain a control log or record showing the date each monitoring device was released from storage, to whom it was assigned, and the date it was returned to storage. The monitoring device will be returned promptly to the designated custodian after its authorized use. A trained agent is required to download the recordings because the devices cannot be connected to the NOC machines.

(6) The Chief, CI, will develop and administer programs to ensure that all employees who operate or install non-telephonic consensual monitoring equipment and pen registers are adequately trained in the use and installation of this equipment. These programs should also ensure that these employees are fully familiar with Federal law, IRS policy, and CI guidelines on the interception of voice communications.

(7) Only those criminal investigators who have attended training programs in the use, operation, and installation of sensitive equipment (except in-line recording devices, or similar devices) will be permitted to install and operate such equipment unless, in emergency situations, another individual is specifically

authorized to do so by the SAC, or designee. Training for this type of equipment will be conducted with sufficient frequency to assure that operators and installers of the equipment retain their expertise.