MANUAL TRANSMITTAL

9.4.6

Department of the Treasury
Internal Revenue Service

SEPTEMBER 3, 2020

EFFECTIVE DATE

(09-03-2020)

PURPOSE

(1) This transmits IRM 9.4.6, Surveillance and Non-Consensual Monitoring.

MATERIAL CHANGES

(1) Exhibit 9.4.6-2, Preservation Letter and any references to it has been deleted to protect Personally Identifiable Information (PII) and/or Federal Tax Information (FTI).

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 9.4.6, July 3, 2013. This IRM was reviewed to ensure content is free from Personally Identifiable Information (PII) and/or Federal Tax Information (FTI), as implemented by the Director, Privacy Policy and Compliance Privacy, Governmental Liaison and Disclosure (PGLD), guidance memorandum dated: April 27, 2020, [Subject: “PII and FTI Review of current Internal Revenue Manuals (IRMs)”].

AUDIENCE

CI

James C. Lee FOR
Don Fort
Chief, Criminal Investigation

9.4.6
Surveillance and Non-Consensual Monitoring

Table of Contents

9.4.6.1
(09-05-2008)
Overview

(1) Enforcement activities include a wide spectrum of Criminal Investigation (CI) activities. Surveillance is an enforcement technique used to obtain information, leads, and evidence. Criminal Investigation surveillance techniques include the following types of surveillance:

a. physical/visual
b. electronic
c. internet
d. video
e. aerial surveillance

9.4.6.2
(09-05-2008)
General

(1) The following applies to CI physical/visual surveillance techniques:

a. Surveillance may be conducted as part of a subject, primary, or general investigation.
b. A journeyman level special agent (GS-1811-12 and above) may conduct surveillance as deemed necessary. A special agent below the journeyman level must obtain prior approval from the Supervisory Special Agent (SSA) for all surveillance activity except under those circumstances where immediate surveillance is necessary and the SSA cannot be contacted. In such instances, the special agent should advise the SSA as soon as practicable of the circumstances that precluded obtaining prior approval.
c. If, during the surveillance, the special agent must assume an identity other than his/her own requiring cover documents, approval for use of these documents must be obtained from the Director, Field Operations or his/her designee (see LEM 9.14.3, Undercover Operations).
d. Surveillance conducted in a high crime area, either on foot or in a vehicle, requires the participation of at least two special agents. Surveillance requiring the use of a vehicle should be conducted in a government owned vehicle that has two-way radio equipment.

9.4.6.2.1
(07-03-2013)
Documentation of Surveillance Activity

(1) The following documentation is required:

a. Surveillance Checklist (see subsection 9.4.6.5).
b. Risk Assessment (see subsection 9.4.6.6).
c. Daily notes of pertinent surveillance activity must be prepared by all participants.
d. Written summary of daily notes must be prepared at the completion of surveillance.

9.4.6.2.2
(09-05-2008)
Reasons for Conducting Surveillance

(1) The following are some of the reasons for conducting surveillance:

a. to obtain evidence of a crime or to identify persons who have indicated they have committed or intend to commit a crime, or who may be involved in the crime being investigated
b. to locate persons by watching locations and associates historically visited by the subject of the surveillance
c. to obtain detailed information about a subject's activities
d. to corroborate the reliability of informants
e. to locate hidden property
f. to obtain probable cause necessary to secure a search warrant
g. to obtain information for later use in interrogations or interviews

h. to develop leads and information received from other sources
i. to know, at all times, the whereabouts of an individual

9.4.6.3
(09-05-2008)
Surveillance and Undercover Distinguished

(1) It is important to distinguish between those investigative techniques which are used in surveillance activities and those which may be utilized during certain undercover operations.

9.4.6.3.1
(09-24-2003)
Surveillance Characteristics

(1) The following characteristics apply to surveillance activities.

a. The purpose is to observe ongoing activities and individuals.
b. Interaction with subjects and third parties is usually not initiated.
c. Conversations are incidental to the surveillance.
d. Conversations are not monitored or recorded.
e. The special agent has limited cover. The purpose of the cover is to protect the integrity of the surveillance.
f. Local special agents are used.
g. Special agents need not be trained in undercover techniques.
h. See subsection 9.4.6.8 concerning internet surveillance.

(2) Surveillance activity bears little resemblance to an undercover operation. The following situations indicate the surveillance activity has evolved into an undercover operation:

a. reliance on cover identities increases
b. contacts with subjects and other individuals are more in-depth
c. agents become participants, rather than mere observers of the activities of interest

(3) The SAC is responsible for ensuring surveillance activities do not evolve into undercover operations without first obtaining the authorization set forth in IRM 9.4.8, Undercover Operations.

9.4.6.3.2
(09-24-2003)
Undercover Operation Characteristics

(1) The following characteristics apply to undercover operations:

a. The purpose is to initiate or participate in activities with identified subjects or objectives.
b. Interaction with subjects and third parties is sought.
c. Undercover agents or other authorized individuals initiate and direct conversations to further the objectives of the operation.
d. Conversations may be monitored and recorded.
e. A covert identity is required to obtain evidence. This cover is used as a basis for contacts with targets or witnesses. However, the lack of a documented cover does not mean the activities engaged in do not constitute an undercover operation.

9.4.6.4
(09-05-2008)
Surveillance at Public Meetings

(1) Attendance at public meetings that promote conduct in violation of the Internal Revenue Code is to be distinguished from attendance at peaceful demonstrations in general opposition to the Sixteenth Amendment. Treasury Department policy directs that no information should be collected at peaceful demonstrations which involve the exercise of First Amendment rights without first contacting the office of the Treasury Under Secretary for Enforcement. In such

situations, the SAC, with the concurrence of the Director, Field Operations will notify the Chief, CI, who will contact the Treasury Under Secretary for Enforcement.

(2) At those public meetings that actually promote conduct in violation of the Internal Revenue Code, surveillance activities will be limited to:

a. identifying the leading figures at the meeting
b. obtaining information concerning methods used to violate tax laws

(3) Special agents may identify those individuals who attend such meetings and who admit or indicate they:

a. have committed or intend to commit a tax violation or other crime
b. advocate that others commit violations of the tax law or commit other crimes
c. advocate the use of threats or assault tactics in dealing with IRS personnel or other Federal, state, or local law enforcement personnel

(4) An example of an appropriate surveillance technique for identifying individuals who attend public meetings and either admit or advocate the violation of laws, or otherwise express an intent to do so, is as follows:

An unidentified member in the audience at a public meeting states that he/she has not filed Federal income tax returns for several years and never intends to file such returns again. Special agents may observe this person enter an automobile and record the license plate number on the automobile in order to attempt to properly identify him/her. If there is a likelihood the individual is driving a borrowed or leased automobile, or is riding with someone else, the agents may continue the surveillance in an attempt to establish a positive identification.

9.4.6.4.1
(09-24-2003)
Public Meetings Defined

(1) The following criteria may be considered to determine whether or not a meeting is public:

a. where the meeting will be held
b. if members of the press will be present or involved
c. if there are any unreasonable restrictions upon entry
d. if public notice of the meeting has been given

9.4.6.4.2
(09-24-2003)
Recording The Proceedings Of Public Meetings

(1) Recording the proceedings of a public meeting is a permissible means of surveillance.

(2) Consensual monitoring authorization must be obtained pursuant to IRM 9.4.7, Consensual Monitoring.

9.4.6.5
(03-02-1999)
Surveillance Checklist

(1) The surveillance team leader is responsible for reviewing the surveillance checklist. If the surveillance involves an undercover operation, refer to the applicable undercover checklist.

9.4.6.6
(07-03-2013)
Risk Assessment Guide

(1) A risk assessment should be completed to assess the potential risk of the surveillance activity. The risk assessment should be discussed with the surveillance team prior to the surveillance.

(2) The assigned special agent should comment on each of the considerations set forth in the risk assessment guide and record the level of risk (low, medium, or high) associated with each consideration.

(3) The SSA and the SAC must review the completed risk assessment guide to determine if the operation can be accomplished safely.

(4) If the operation cannot be accomplished safely, the special agent should abandon any further planning activity.

(5) All approved risk assessment forms should be maintained in the investigative folder or filed electronically.

9.4.6.7
(09-24-2003)
Electronic Surveillance

(1) The following subsections refers to electronic surveillance and the monitoring of electronic communications.

9.4.6.7.1
(09-05-2008)
General

(1) The "Electronic Communications Privacy Act" (ECPA) of 1986, Pub. L. No.99-508, 100 Stat.1848, amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC §2510 et. seq.). This legislation significantly revised Title III to reflect technological advances in electronic communications. It also added provisions: (1) specifying how government entities may obtain access to stored electronic communications; and (2) updating the provisions relating to pen registers and trap-and-trace devices. The ECPA provisions amended or modified the following statutes:

a. Title I-Interceptions of Communications and Related Matters (codified in 18 USC §2510 et. seq.). As originally enacted, the wiretap statute regulated the real-time acquisition of "wire" and "oral" communications. A "wire communication" is the transmission of human voice over a "wire" (" telephone circuit") or other means of electronic communication. An "oral communication" is a conversation between or among individuals in circumstances in which there exists an expectation that the communication will not be "intercepted." The ECPA added " electronic communications" to the wiretap statute and provided slightly different rules for obtaining orders for the real-time acquisition of such communications.
b. The ECPA provides rules for the real-time acquisition of wire, oral, or electronic communications, as well as the acquisition of stored wire and electronic communications (see subsection 9.4.6.7.3).

(2) Orders for real time interceptions (i.e., "wiretaps") have traditionally been referred to as "Title IIIs" or "T-IIIs" because the authority to obtain such orders originated in Title lll of the Omnibus Crime Control and Safe Streets Act of 1968. This section refers to such orders simply as "wiretap" orders.

a. Title II-Stored Wire and Electronic Communications and Transactional Records Access (codified in 18 USC §2701 et. seq.).
b. Title III-Pen Registers and Trap-and-Trace Devices (codified in 18 USC §3121 et. seq.).
c. On October 25, 1994, Congress enacted the Communications Assistance for Law Enforcement Act, Pub. L. 103-414, Oct. 25, 1994, which amended certain provisions of Titles I, II, and III of ECPA and became effective on January 6, 1995. The Communications Assistance for Law Enforcement Act is intended to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept commu-

nications involving advanced technologies (e.g., digital or wireless transmission modes), or features and services (e.g., call forwarding, speed dialing and conference calling), while protecting the privacy of communications and without impending the introduction of new technologies, features, and services. To guarantee that law enforcement agencies can continue to conduct authorized interception in the future, the Communications Assistance for Law Enforcement Act requires telecommunications carriers to ensure that their systems have the capability to: (1) isolate the content of targeted communications transmitted by the carrier within the carrier's service area; (2) isolate the information identifying the origin and destination of targeted communications; (3) provide intercepted communications and call identifying information to law enforcement agents so they can be transmitted over lines or facilities leased by law enforcement agents to a location away from the carrier's premises; and, (4) carry out interceptions unobtrusively, so targets are unaware of the interception and in a manner which does not compromise the privacy and security of other communications. The Communications Assistance for Law Enforcement Act allows the industry to develop the standards to implement the equipment.

d. On October 25, 2001, Congress passed the United Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, Pub.L. 107-56, Oct. 25, 2001, which became effective on October 26, 2001. The purpose of the USA Patriot Act is to deter and punish domestic and international terrorist acts, as well as to enhance law enforcement investigatory tools. Title II (Enhanced Surveillance Procedures) of the USA Patriot Act amends certain provisions of ECPA, the Communications Assistance for Law Enforcement Act and 18 USC Chapters 119 (Wire and Electronic Communications Interception of Oral Communications), 121 (Stored Wire and Electronic Communications and Transactional Records Access) and 206 (Pen Registers and Trap and Trace Devices.

(3) Interception of wire, oral, or electronic communications without the consent of a party to the communication.

a. Non-consensual Monitoring of Oral and Wire Communications - The non-consensual interception of oral and wire communications is restricted to those investigations which involve the felonies listed in 18 USC §2516. Although, that section does not refer to tax crimes, the felonies listed therein include 18 USC §1956 and 18 USC §1957 (money laundering offenses), and certain offenses for which 31 USC §5322 provides the criminal penalties related to currency reporting offenses. IRS policy therefore restricts the use of non-consensual interception of oral and wire communications to "extremely limited situations" and only in "significant money laundering investigations."

b. Non-consensual monitoring of Electronic Communications - 18 USC §2516(3) authorizes the real time interception of electronic communications to investigate any Federal felony.

c. Access to Stored Electronic Communications -18 USC §2703 specifies the means by which law enforcement (government) may obtain access to stored electronic communications and transactional records.

d. Title 18 USC §3122 authorizes the use of pen registers and trap and trace devices for investigations of all Federal felonies.

9.4.6.7.1.1
(07-03-2013)
Restrictions on Electronic Surveillance Techniques

(1) The permanent installation of concealed microphones, recording equipment, and similar devices in IRS offices is prohibited. Temporary installations are permitted only when authorized in accordance with the requirements for consensual and non-consensual monitoring.

(2) The use of transmitters or other devices used to assist in trailing vehicles or personal property is permitted pursuant to subsection 9.4.6.7.5 and 18 USC §3117.

(3) Although mechanical devices may be used to intercept, overhear, or record conversations at public telephones, pursuant to the procedures outlined in 18 USC §2510, et seq., extreme care must be exercised to segregate conversations of innocent third parties from conversations of the identified subject(s). In each instance of monitoring, the equipment must be installed immediately prior to monitoring the identified subject and removed immediately thereafter. Due to the potential for inadvertent monitoring of innocent third party conversations and the elevated standard of probable cause required for this type of monitoring, it is rarely used; however, extreme caution should be exercised when this technique is utilized.

(4) Miniature recorders and radio transmitters will not be used surreptitiously in conducting routine surveys and interviews with third parties unless consensual monitoring is authorized.

(5) Field offices may not purchase, fabricate, or arrange for the manufacture of any equipment or accessories designed to acquire communications of any type without obtaining approval from the Associate Director, Security and Technical Operations or his/her designee. The acquiring field office shall enter all such equipment into the Criminal Investigation Management Information System (CIMIS).

(6) Permission to employ eavesdropping devices may only be granted to special agents or to personnel acting under their direction. The approval process, prohibitions, and limitations outlined in this section apply equally to non-IRS personnel who act at the direction of special agents.

(7) Title 18 prohibits the use of radio scanners to listen to transmissions on wireless telephone frequencies (e.g., mobile telephones or cordless telephones). Monitoring of wireless transmissions requires a wiretap order pursuant to 18 USC §2518. Normally, citizens band radio transmissions may be monitored unless there is reason to believe that a base station is using a wire link supplied by a common communications carrier.

(8) A search warrant issued pursuant to Rule 41, Federal Rules of Criminal Procedure, is required to obtain evidence that cannot be observed from a public place with the naked eye. Federal statutes and the Supreme Court have placed restrictions on the use of sense enhancing devices. The local Criminal Tax attorney should be consulted prior to the use of such technology.

9.4.6.7.2
(09-05-2008)
Real Time - Interceptions of Communications and Related Matters

(1) The “wiretap statute”, 18 USC §2510 et. seq., governs the interception of wire, oral, and electronic communications in transmission (i.e., “real-time” interceptions) through the use of electronic, mechanical, or other devices.

9.4.6.7.2.1
(09-05-2008)
Definitions

(1) *Contents* are defined by 18 USC §2510(8) to include any information concerning the substance, purpose, or meaning of any given communication.

(2) A *wire communication* is defined as a communication that involves the human voice being transmitted through the use of a wire, cable, or similar method between the points of origin and reception (see 18 USC §2510(1) and (18).) In addition, tone-and-voice pagers are included within the definition of a wire communication, and the interception of the human voice segment must be treated the same as a wire interception. A conversation on a telephone is a wire communication.

(3) An *oral communication* is "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectations, but this term does not include any electronic communication." A conversation between two or more individuals who have a reasonable expectation that the conversation will not be intercepted constitutes an oral communication.

(4) An *electronic communication* is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system that affects interstate or foreign commerce." The term electronic communication does not include communications containing the human voice. An electronic communication includes the "real-time" point-to-point transmission of, for example, digital display pager information, electronic mail, computer-to-computer transmissions, facsimiles, transmissions, and private video transmissions (but not video surveillance).

(5) *Interception* means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use on any electronic, mechanical, or other device."

(6) *Electronic, mechanical or other device* is defined by 18 USC §2510(5) to include "any device or apparatus which can be used to intercept a wire, oral or electronic communication other than." Examples of such a device or apparatus include:

a. Any telephone or telegraph instrument, equipment or facility, or any component thereof (i) furnished to the subscriber or user by a provider of wire or electronic communication service and used by the subscriber or user...in the ordinary course of its business or (ii) being used by a provider...in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of his duties.
b. A hearing aid or similar device being used to correct subnormal hearing to no better than normal.

Note: Merely overhearing a conversation by listening in on an extension telephone or using a "normal" hearing aid is outside the definition of an interception because the telephone set and hearing aid are excluded from the definition of an "electronic or mechanical device."

(7) Consent is defined to mean that one or more of the parties to a wire, oral, or electronic communication has given his/her prior permission that such communication may be intercepted. In the Federal system, one party's consent is needed, even if the other parties to the conversation are unaware that the communication is being intercepted or recorded.

9.4.6.7.2.2
(09-05-2008)
Access to "Real-Time" Oral Communication - Wiretaps

(1) A "wiretap" is the acquisition of the contents of a wire or oral communication through the use of any electronic, mechanical, or other device where an expectation exists that the communication is not subject to interception. See subsection 9.4.6.7.1(3)(a) for a discussion of those offenses for which wiretaps may be authorized.

(2) The following are not covered by the wiretap statute:

a. use of pen registers or trap and trace devices; authority for the use of these techniques is found in 18 USC §3122
b. overhearing of conversations without the aid of electronic, mechanical, or other devices
c. radio or television broadcasts readily accessible by the public
d. tone-only pagers per 18 USC §2510 (12)(B)
e. electronic tracking devices, also called transponders or beepers (18 USC §3117)
f. marine and aeronautical communication systems per 18 USC §2511(2)(g)(ii)(IV)
g. public safety radio systems
h. amateur radio operator services, citizens band radio, and general mobile radio services
i. electronic communications which are readily accessible by the general public
j. physical/visual surveillance
k. individuals' use of telephone extensions

(3) Consensual monitoring where one of the parties consents to the monitoring of the conversation or internet communication is addressed and specifically excepted out of the wiretap statute.

9.4.6.7.2.3
(09-05-2008)
Disclosure and Derivative Use Orders

(1) An order to intercept wire, oral, or electronic communication may be obtained only to investigate those offenses enumerated in 18 USC §2516 (Title 26 offenses are not included). However, if the contents of intercepted wire, oral, or electronic communications relate to other criminal acts, that evidence may be used by other law enforcement officers (including CI special agents) in furtherance of their investigations, including Title 26 offenses. Title 18 USC §2517 sets forth a statutory scheme under which the disclosure and use of intercepted oral, wire, or electronic communications is permitted.

(2) Title 18 USC §2517(1) permits law enforcement officers (obtaining officers) who obtain intercepted wire, oral, or electronic communications to disclose such evidence to other law enforcement officers (receiving officers) as is appropriate in the performance of the obtaining and receiving officers' duties.

(3) Title 18 USC §2517(2) permits law enforcement officers who have lawfully obtained or received intercepted wire, oral, or electronic communications, or evidence otherwise derived from intercepted wire, oral, or electronic communications, to use the contents of that evidence to the extent such use is appropriate for the proper performance of his/her official duties.

(4) Title 18 USC §2517(3) permits law enforcement officers who have obtained or received information from intercepted wire, oral, or electronic communications, or evidence otherwise derived from intercepted communications, to disclose such information while giving testimony under oath in any Federal or state, criminal, or civil proceeding. This includes testimony before a grand jury.

(5) Title 18 USC §2517(5) requires that a court order, referred to as a "derivative use order," be obtained prior to any disclosure as defined in 18 USC §2517(3), of intercepted communications relating to offenses other than those specified in the order of authorization or approval to intercept. Such an order must be obtained prior to any law enforcement officer making any testimonial disclosure of information or evidence relating to intercepted wire, oral, or electronic communications, or evidence derived from such intercepted communications. Such an application should be made as soon as practicable. The derivative use order must be based upon the court's finding that the information and evidence to be disclosed was otherwise properly intercepted. Failure to obtain such an order can result in the dismissal of the case or subject the officer to liability for civil damages related to the unauthorized disclosure.

9.4.6.7.2.4
(09-05-2008)
Evaluation of Wiretap Information

(1) As soon as practicable, information or evidence received by CI special agents from other law enforcement officers that originated from intercepted wire, oral, or electronic communications, or evidence otherwise derived from the intercepted communications or transcripts thereof, will be referred to the SAC, or his/her designee, who should immediately evaluate the potential use for criminal and civil tax purposes.

(2) If it is apparent that the information or evidence is likely to or will be used by IRS in a criminal or civil judicial proceeding, the SAC, or his/her designee, should immediately ascertain whether an 18 USC §2517(5) order covering use by the IRS has been obtained. If an order has not yet been obtained, the SAC or his/her designee should contact and consult with the supervisory Assistant United States Attorney (AUSA) to ensure the order is obtained prior to disclosure.

9.4.6.7.2.5
(09-24-2003)
Wiretap Approval Process

(1) Three situations exist where approval is required for IRS CI special agents' participation in investigations where non-consensual monitoring of voice communications occurs:

a. When CI special agents are present in the wire room and do NOT have the responsibility of monitoring conversations as they occur.
b. Criminal Investigation monitoring of non-consensual conversations where an agent from another agency prepared the affidavit in support of an application for monitoring.
c. Criminal Investigation monitoring of non-consensual conversations where an agent from CI prepared the affidavit in support of an application for monitoring.

9.4.6.7.2.5.1
(09-05-2008)
Criminal Investigation Special Agents Present in the Wire Room, but DO NOT have the Responsibility of Monitoring Conversations

(1) IRS CI special agents can provide valuable assistance in some investigations using the non-consensual monitoring technique where the assistance **DOES NOT** involve the real-time monitoring of conversations. The duties may require a scheduled presence in the wire room and require significant resources. The duties include oversight of occurring activity, issuing surveillance assignments, reviewing previously recorded conversations, etc.

(2) Approval of these situations is required in writing by the SAC and must address the significance of the investigation, any issues concerning staffing needs, and any CI equipment to be used during the operation.

9.4.6.7.2.5.2
(07-03-2013)
Criminal Investigation Monitoring of Non-Consensual Conversations When Criminal Investigation IS NOT the Affiant Agency

(1) A copy of the affidavit and a memorandum from the field office through the Director, Field Operations to Special Investigative Techniques is required. Prior to the memorandum being sent officially to Special Investigative Techniques and through the agent's chain of command, the preparing agent should contact a senior analyst in Special Investigative Techniques responsible for the T-III program for vetting of the memorandum. The memorandum must include the following information:

a. The complete background of the investigation, including the other participating Federal, state and local law enforcement agencies involved in the investigation. The name of the criminal organization and the criminal offenses which are being investigated.
b. The significance of the target, organization, or compliance problem being investigated. The type of phone line, telephone number(s) to be monitored, and subscriber information should also be mentioned (e.g., telephone line, cellular telephone, etc.).
c. Financial information (e.g., how the organization launders proceeds amount of money being wired, increments, and currency seized to date).
d. Why CI participation in the monitoring is necessary (e.g., due to the volume of calls, or CI has the financial expertise to analyze the information as it is being received to prevent minimization of conversations that other officers or agents might not properly recognize as being material to the financial aspects of the investigation).
e. The amount of CI resources needed. This number should include separate categories covering the number of special agents actually monitoring the calls and the number of special agents who will assist in surveillance or related support duties.

(2) Upon receipt of the affidavit and memorandum, Special Investigative Techniques will prepare a request for the concurrence of the Chief, CI, and a routing slip seeking the approval from the Deputy Commissioner, IRS.

9.4.6.7.2.5.3
(07-03-2013)
Criminal Investigation Monitoring of Non-Consensual Conversations When Criminal Investigation IS the Affiant Agency

(1) A copy of the affidavit and a memorandum from the field office, through the Director, Field Operations, to Special Investigative Techniques is required prior to obtaining the court order. Prior to the memorandum being sent officially to Special Investigative Techniques and through the agent's chain of command, the preparing agent should contact a senior analyst in Special Investigative Techniques responsible for the T-III program for vetting of the memorandum. The memorandum must include the following information:

a. The complete background of the investigation, including the other participating Federal, state and local law enforcement agencies involved in the investigation. The name of the criminal organization and the criminal offenses which are being investigated.
b. The significance of the target, organization, or compliance problem being investigated.
c. The type of phone line, telephone number(s) to be monitored, and subscriber information should be mentioned (e.g., telephone line, cellular telephone, etc.).
d. Financial information (e.g., how the organization launders proceeds (amount of money being wired, increments, and currency seized to date).
e. The opinion and any recommendations from the field office's Criminal Tax attorney.
f. Why CI participation in the monitoring is necessary, such as CI has the financial expertise to analyze the information as it is being received to

prevent minimization of conversations that other officers or agents might not properly recognize as being material to the financial aspects of the investigation.

g. The amount of CI resources needed should be listed in the memorandum. This number should include separate categories covering the number of special agents actually monitoring the calls and the number of special agents who will assist in surveillance or related support duties.

(2) Upon receipt of the affidavit and memorandum, Special Investigative Techniques will forward the affidavit to Division Counsel/Associate Chief Counsel (Criminal Tax) seeking their advice. Special Investigative Techniques will prepare a request for the Chief, CI's, concurrence and a routing slip seeking the approval from the Deputy Commissioner, IRS.

9.4.6.7.2.6
(07-03-2013)
Reports, Extensions, Expansions and Closing Reports Related to Wiretaps When CI Special Agents Are Actively Monitoring Conversations

(1) Copies of the 10-day reports and closing reports must be sent to Special Investigative Techniques within 15 days of the completion of the report.

(2) If an extension of time is required, the Director, Field Operations is the approving official. A request must be prepared by the field office providing a summary of the results obtained to date and a reason for the extension. Upon approval by the Director, Field Operations, the request will be electronically forwarded to Special Investigative Techniques.

(3) If an expansion is required to add new telephone lines related to the same targets and the same offenses, the Director, Field Operations is the approving official. A request must be prepared by the field office providing a summary of the results obtained to date and a reason for the expansion. Upon approval by the Director, Field Operations, the request will be electronically forwarded to Special Investigative Techniques.

(4) If it becomes necessary to include additional targets or additional offenses, approval by the Deputy Commissioner, IRS is required. The procedures for the expansion to add new targets or add new offenses mirrors the procedures required to initiate a wiretap request (see subsections 9.4.6.7.2.5.2 or see 9.4.6.7.2.5.3).

9.4.6.7.2.7
(09-05-2008)
Access to "Real Time" Electronic Communications

(1) The "real time" or simultaneous interception of digital display pagers in transmission, transmission of electronic mail, computer-to-computer transmissions, facsimile transmissions, and private video transmissions (but not video surveillance) are all covered by the wiretap statute (see subsection 9.4.6.7.2.1 - stored electronic communications 18 USC §2703.)

(2) The interception of electronic communications can provide valuable information and evidence relating to any Federal felony under the investigative jurisdiction of CI, including Title 26 offenses. Under 18 USC §2516(3), the order authorizing such interception must conform to 18 USC §2518. However, cost, technical requirements, and encryption are all factors that can impact its actual use.

9.4.6.7.2.7.1
(07-03-2013)
Approval/Authorization for "Real Time" Electronic Communications

(1) Prior to seeking a wiretap order for electronic communications, the special agent must prepare an affidavit for the application and a memorandum seeking approval. Both must be forwarded from the SAC, through the Director, Field Operations, to Special Investigative Techniques. The field office Criminal Tax attorney and the Computer Telecommunications Coordinator (CTC) in the local

United States Attorney's office should be contacted for assistance in preparing those documents. The memorandum must include the following information:

a. The complete background of the investigation, including the other participating Federal, state and local law enforcement agencies involved in the investigation. The name of the criminal organization and the criminal offenses which are being investigated.
b. The significance of the target, organization, or compliance problem being investigated.
c. Specific description of the device(s) that the field office intends to monitor.
d. Financial information, e.g., how the organization launders proceeds, how tax evasion is being promoted, and/or the scope of the problem.
e. The opinion, and any recommendations from, the field office's Criminal Tax attorney.
f. Why CI participation in the monitoring is necessary, e.g., CI has the financial expertise to analyze the information as it is being received to quickly respond to financial transactions as they occur or the details of complex transactions can only be obtained through the computer information since the financial activity is conducted offshore.
g. The amount of CI resources needed should be listed in the memorandum.

(2) Upon receipt of the affidavit and memorandum, Special Investigative Techniques will review the request and forward it to the Director, Operations Policy and Support for approval.

9.4.6.7.2.7.2
(07-03-2013)
Reports, Extensions, Expansions and Closing Reports Related to "Real Time" Access of Electronic Communications

(1) Following approval to seek a wiretap order, copies of the 10-day reports and closing reports must be sent to Special Investigative Techniques.

(2) If an extension of time is required, the Director, Field Operations is the approving official. A request must be prepared by the field office providing a summary of the results obtained to date and a reason for the extension. Upon approval by the Director, Field Operations, the request will be electronically forwarded to Special Investigative Techniques.

(3) If an expansion is required to add new internet sites or e-mail accounts related to the same targets and the same offenses, the Director, Field Operations is the approving official. A request must be prepared by the field office providing a summary of the results obtained to date and a reason for the expansion. Upon approval by the Director, Field Operations, the request will be electronically forwarded to Special Investigative Techniques.

(4) The same procedures used to initiate a request must be followed to add targets or offenses to a wiretap order. Such expansion requests must be approved by the Director, Operations Policy and Support.

9.4.6.7.3
(09-05-2008)
Stored Wire and Electronic Communications

(1) Title 18 USC §2701 et. seq., specifies how governmental entities may obtain access to stored electronic communications, transactional records, and subscriber records.

9.4.6.7.3.1
(09-24-2003)
Stored Electronic Communication/ Transactional Information/Subscriber Information

(1) Stored electronic communications (defined in 18 USC §2510) includes those electronic messages temporarily stored by an electronic communications service provider prior to delivery to the intended recipient or stored as a backup. The term also includes information stored with a " remote computing service". The term includes display data stored in digital-display pagers and cell phones, stored electronic mail, stored computer-to-computer transmissions, stored telex transmissions, stored facsimile data, and private video transmissions.

(2) The statute applies only to data stored with an electronic communications service provider. The real-time interception of transmissions to tone-and-voice-pagers is governed by the wiretap statute. (A tone-and-voice-pager enables callers to transmit short voice messages to a subscriber's pager). The acquisition of transmissions to or from display pagers and facsimile transceivers during the transmission(s) requires the approval of the Deputy Commissioner, IRS, an affidavit, an application (which must be approved by the Department of Justice), and a court order obtained in accordance with 18 USC §2516 and §2518 (see subsection 9.4.6.7.2.7).

9.4.6.7.3.2
(09-05-2008)
Disclosure of Stored Communications

(1) Title 18 USC §2702 prohibits disclosure of electronic communications by providers of electronic communication services or remote computing services unless one or more of the following conditions is met:

a. the information is given to its intended recipient or addressee
b. the information is given to the government pursuant to a court order, search warrant, or subpoena
c. the subscriber/customer gives consent
d. the disclosure is to a facility used to forward the communication
e. the disclosure is incident to testing equipment or quality of service
f. the information was obtained inadvertently and specifically refers to a crime

(2) Title 18 USC §2702(c)(4) permits, but does not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an eminent act which could result in the death of or cause serious physical injury to any person as provided by the USA Patriot Act.

9.4.6.7.3.3
(09-03-2020)
Judicial Process for Obtaining Stored Electronic Communications, Transactional Information, and Subscriber Information

(1) Title 18 USC §2703 specifies the means by which a governmental entity may obtain access to stored electronic communications. The statute prohibits electronic communications providers from voluntarily providing information to a governmental entity, and requires law enforcement to use either a search warrant, court order, or subpoena (as described below in paragraphs 2, 3, 4, and 5) in order to obtain the following classes of information:

a. The contents of electronic communication in electronic storage with an electronic communication service (such as unopened e-mail) or with a remote computing service (such as records in off-site archives).
b. Basic subscriber information; including the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity (such as temporarily assigned Internet Protocol (IP) addresses); length of service; and types of services the customer or subscriber utilized.

c. Transactional information, which includes all other records or information pertaining to a subscriber or customer that are not included in a) or b).

(2) If the contents of a wire or electronic communication have been in storage for 180 days or less, the government must obtain a search warrant, based on probable cause, to obtain access to the contents. Notice to the subscriber or customer is not required. Because the statute requires the use of a search warrant to obtain this class of information, it is not necessary to prepare an Enforcement Action Approval Form or to justify the use of the warrant as the least intrusive means to obtain the Information. Form 9809, Request for Stored Electronic Information is used to obtain the appropriate authorization for the search warrant application and execution.

a. The government may obtain the contents of an electronic communication that has been in storage for more than 180 days using a search warrant, a court order issued under 18 USC §2703(d), or a grand jury subpoena or administrative summons.
b. Notice need not be given to the subscriber if a search warrant is used to obtain the information. The statute requires that the customer or subscriber to whom the information pertains be notified if the government obtains a court order or issues a subpoena or summons for the information. That notice may be delayed for up to ninety days pursuant to 18 USC §2705. (This initial 90-day period can be extended for an additional 90-day period upon application to the court for an extension under 18 USC §2705(4).) Exhibit 9.4.6-1 is a sample of a 18 USC §2703(d) Order.

(3) The above-stated transactional information may be obtained, without providing notice to the subscriber, by any of the following means:

a. A search warrant.
b. A court order for disclosure per 18 USC §2703(d).
c. Consent from the customer or subscriber of the service.
d. Submission of a formal written request, pursuant to a law enforcement investigation concerning telemarketing fraud, for the name, address, and place of business of a subscriber or customer of such provider, when a subscriber or customer is engaged in telemarketing as defined in 18 USC §2325.

Note: At least one Circuit Court of Appeals has found portions of the Stored Communications Act (SCA) that permit the obtaining of e-mails pursuant to subpoena or court order unconstitutional. Thus, a search warrant may be required notwithstanding the language of the SCA or this IRM. Where the obtaining of e-mails by subpoena or court order is contemplated, consult with a local CT Attorney before proceeding.

(4) Basic subscriber information may be obtained with any of the means described in (3) above or with a grand jury subpoena or administrative summons, without providing notice to the subscriber.

(5) Title 18 USC §2703(f) imposes on the provider of wire or electronic communication services or a remote computing service the obligation, upon the written request of a governmental entity, to take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

a. The Preservation Letter requires providers of wire or electronic communication services or remote computing services to retain records for a period of 90 days. This initial 90-day period can be extended for an additional 90-day period upon a renewed request by the governmental entity.

9.4.6.7.3.4
(07-03-2013)
Approval/Authorization for Stored Electronic Communications, Transactional Information, and Subscriber Information

(1) The investigating special agent should consult with the local Computer Investigative Specialist (CIS) and Criminal Tax attorney about access to stored electronic or wire communications to determine the proper method of obtaining the desired information. The use of court orders and search warrants to obtain stored electronic information, transactional information, or subscriber information requires approval by the SAC on Form 9809. After SAC approval, the Form 9809 must be forwarded electronically to Special Investigative Techniques for filing. The SAC must seek the endorsement of the United States Attorney to apply for a court order to obtain stored electronic communications. Local procedures must be followed to obtain the court order. If preparation of an affidavit is necessary, the local Criminal Tax attorneys opinion regarding the affidavit's legal sufficiency and form should be obtained. The SAC approval is not required when a subpoena is used for obtaining the information.

Note: At least one Circuit Court of Appeals has found portions of the Stored Communications Act (SCA) that permit the obtaining of e-mails pursuant to subpoena or court order unconstitutional. Thus, a search warrant may be required notwithstanding the language of the SCA or this IRM. Where the obtaining of e-mails by subpoena or court order is contemplated, consult with a local CT Attorney before proceeding.

9.4.6.7.3.5
(09-05-2008)
Closing Reports for Stored Electronic Communications/ Transactional Information/Subscriber Information

(1) In situations where a court order or search warrant was used, a memorandum will be submitted to CI:OPS:SIT. The memorandum is due 15 working days after receipt of the information by the field office. The memorandum should contain information identifying the investigation name and number, the allegations involved, the reason the information was acquired, and a description of the information obtained.

9.4.6.7.4
(09-05-2008)
Pen Registers and Trap and Trace Devices

(1) Devices connected to telephone circuits may be used to obtain the telephone numbers dialed by a target telephone (pen register) or the telephone number dialing the target telephone (trap-and-trace devices). The acquisition of dialed numbers is governed by 18 USC §3121 thru §3126. Title 18 USC §3121 was amended by the USA Patriot Act to prohibit obtaining contents of any wire or electronic communication via pen register or trap and trace device.

(2) Pen registers and trap-and-trace devices are subject to Fourth Amendment requirements when physical intrusion is needed for the installation of such devices. Limited entries to install this equipment are permitted provided they are done pursuant to a valid search warrant.

9.4.6.7.4.1
(09-05-2008)
Use of Pen Registers

(1) A pen register, which is more appropriately called a ″Dialed Number Recorder″ (DNR), is a mechanical instrument attached to a telephone line, usually at a central telephone office. A pen register:

a. records the outgoing numbers dialed on a particular telephone
b. registers incoming calls
c. does not identify the telephone number from which the incoming call originated unless caller identification (ID) service is present, the service is on, and no one has blocked the caller ID service

(2) Use of pen registers is restricted to recording the area code, telephone number, and extension dialed. Pen registers may not be utilized for gathering transactional data input by a touch-tone phone (i.e., account numbers, amounts, etc.).

(3) If possible, equipment that does not record transactional data should be used. Gathering transactional data input by touch-tone phone constitutes interception of electronic communication in transmission and requires a wiretap order that must be obtained under the procedures in subsection 9.4.6.7.2.

(4) Pen registers and other types of telephone number recorders can be utilized only when authorized by court order, except as provided by 18 USC §3121(b). They may be used in both tax and non-tax investigations where CI has the authority to investigate and locate fugitives from justice who are the subject of a CI investigation. A fugitive from justice is defined as a person against whom criminal action (e.g., return of an indictment, filing of a complaint or information, or a conviction) has been taken, and who has fled the jurisdiction to escape prosecution or to avoid serving a sentence. Requests for pen registers to locate fugitives will be considered only for fugitives who are charged with felony violations.

(5) Unless an exception is approved by the SAC, only IRS-owned pen registers and accessory equipment may be used in CI investigations.

(6) The USA Patriot Act amended 18 USC §3121, §3123, §3124, and §3127 to clarify that the pen register and trap and trace statute applies to a broad variety of communication technologies. As a result, law enforcement may use pen registers and trap and trace device orders to trace communications on the Internet and other computer networks.

(7) The USA Patriot Act added 18 USC §3123(a)(1) which gives Federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

(8) The USA Patriot Act added 18 USC §3123(a)(3) whereby law enforcement authorities are required to file a special report with the court whenever it is necessary to install a separate device, such as Etherpeek or the FBI's DCS 1000, to collect the information sought. The special report must include: the identity of the officers who installed or accessed the device; the date and time the device was installed, accessed, and uninstalled; the configuration of the device at installation with any subsequent modifications; and the information collected by the device.

(9) The USA Patriot Act added 18 USC §3123(b)(1)(C) such that there are no geographic limitations placed upon pen registers and trap and trace devices; thus, pen register and trap and trace orders extend nationwide and are not limited to the jurisdiction in which the order was issued. The issuing court must, however, have jurisdiction over the crime under investigation

9.4.6.7.4.2
(07-03-2013)
Request for Approval

(1) The SAC, or his/her designee, will seek the endorsement of the US Attorney to apply for a court order pursuant to 18 USC §3123. Pen registers require approval by the SAC on Form 9170, Request for Pen Register and/or Trap and Trace Devices. After SAC approval, the Form 9170 must be forwarded electronically to Special Investigative Techniques for filing.

(2) Upon final approval by the SAC, the investigating special agent should promptly contact the US Attorney for the purpose of obtaining a court order based upon an application by the AUSA pursuant to 18 USC §3122. (Exhibit 9.4.6-3 Application for Pen Register; Exhibit 9.4.6-4, Court Order for Pen Register). After approval by the magistrate or judge, the SAC, or his/her designee, will arrange for the timely shipment of a pen register(s) and other requested accessory equipment.

(3) Orders pursuant to 18 USC §3123 which authorize the installation of pen registers or trap and trace devices shall also authorize the use of such devices for a period not to exceed 60 days. Extensions for a period not exceeding 60 days are available upon application for another court order pursuant to 18 USC §3122 and 18 USC §3123(C)(1) and (2).

9.4.6.7.4.3
(09-05-2008)
Oral Requests

(1) If time does not permit the completion of Form 9170, the information may be orally transmitted to the SAC. An oral request for approval must be confirmed in writing and submitted within 2 working days after the oral request is made. After the oral approval has been obtained, the investigating special agent will contact the US Attorney to apply for the necessary court order. The previously discussed approval process and routing of the Form 9170 applies.

(2) Title 18 USC §3125 addresses emergency pen register installation prior to obtaining a court order and relates only to those situations involving the immediate threat of death or serious bodily injury, or conspiratorial activities characteristic of organized crime. The local Criminal Tax attorney and AUSA should be consulted to ensure the statute is followed.

9.4.6.7.4.4
(09-05-2008)
Installation of a Pen Register

(1) The intentional installation or use of pen registers or trap and trace devices without first obtaining a court order under 18 USC §3123 is prohibited. In compliance with the prohibition, the following procedures must be completed in order to install a pen register.

(2) Contact the telephone company to identify the line to which the pen register is to be attached.

(3) If the telephone company does not have the personnel available to confirm the correctness of the line at the appearance point, the tech agent will do the following:

a. A voltmeter must be attached to the identified line to determine if the telephone is in use.
b. If the telephone is not in use, attach the telephone test set to the line and confirm that the line is the correct line. If someone attempts to use the line while the butt set is attached to the line, the butt set will be immediately disconnected and not be reconnected until it has been determined (using the voltmeter) that the line is not in use.
c. Note that if physical intrusion is necessary for installation, a search warrant or consent is required.

(4) After the pen register has been activated, the SAC will ensure that installers and operators are competent to operate the equipment. Adequate precautions will be taken to limit access to the pen register only to its operator and other necessary personnel. Upon completion of use, pen registers must be immediately returned to the issuing office.

(5) Pen registers may not be utilized for gathering any transactional data inputted by a touch-tone phone (i.e., account numbers, amounts, etc.).

(6) If the authorization is not utilized, a memorandum will be submitted to the SAC setting forth the reasons for not using the pen register. The memorandum will include the name of the investigations pursuant to which authorization was sought.

(7) If an extension is necessary, submit a request per Form 9170 to the SAC for consideration. The request must summarize the information that has been obtained to date, and set forth the number of days the extension is sought. The extension may not exceed 60 days.

(8) Requests to add additional phone numbers or equipment not specified in the original order must be made per Form 9170 and must set forth the reasons supporting the issuance of another order under 18 USC §3123. Include in the request the new telephone numbers to be monitored and the name(s) and address(es) of the subscribers. The request for an extension of time can be combined with this request where appropriate.

9.4.6.7.4.5
(07-03-2013)
Trap and Trace ("Grabber")

(1) A trap and trace device is also called a ″grabber″. It records the telephone numbers from incoming calls to a particular telephone. The device used by the telephone company is a TTS-176 device, an electronic switching system (ESS), or a cross bar switching facility. Like a pen register, no conversations will be recorded. Trap and trace procedures are necessary when attempting to monitor call forwarding.

(2) Call forwarding is part of the trap and trace procedure. It requires a telephone company to identify which facility or number telephone calls are being forwarded. Historically, telephone companies have been reluctant to assist in trap and trace procedures or call forwarding monitoring unless the situation concerns threats to the President of the United States and/or involves a kidnapping. The statute now protects companies from any liability resulting from the use of such devices (see 18 USC §3124(d)).

(3) The telephone company may be able to provide a record of incoming calls to the telephone of a subject under investigation. This depends on the type of switching facility (exchange) involved. This information can be as useful as a pen register/DNR.

(4) Trap and trace service requires the same approval as pen registers/DNRs. Requests, extensions, and any deviations from requests must conform to the same procedures governing pen register requests and will be considered in the same manner.

(5) Consider the availability and use of ″caller ID″ to obtain desired information prior to applying for a trap and trace authorization.

(6) A court order under 18 USC §3123 is required. This order requires the same application and the same information as the order for installation of pen registers.

(7) Whenever possible, before obtaining an order to trace incoming calls to a particular line, review the proposed trace with the local telephone company's security officer. The security officer should be able to advise of foreseeable problems in the execution of the proposed order.

(8) Except in very rare instances, orders should be limited to Electronic Switching System (ESS) or No. 5 cross-bar facilities. The likelihood of successfully tracing telephone calls through a system using less sophisticated equipment is extremely low and requires an inordinate amount of time and equipment.

(9) Where possible, all orders should also be limited with respect to the following:

a. Scope: An order should minimize the number of lines on which trap and trace service is requested at a given switching facility.
b. Geography: It is preferable that the order limit traces to ″all calls originating in X city″ or ″all calls originating within a y-mile radius of Z town.″
c. Duration: Orders must limit the trace to 60 days, subject to an extension of an additional 60 days if the supervising attorney determines it to be necessary.
d. Hours: If it is possible to anticipate when calls will come into a target phone, tracing should be limited to these hours.

(10) Seek the tracing information from the telephone company no more than once a day and, except in unusual circumstances, only during regular business hours.

(11) Each order should contain a clause forbidding the telephone company to disclose that a trace is or has been in progress as provided by 18 USC §3123(d). A telephone company should be given the opportunity for a closed hearing before the issuing judge to seek limitations of any proposed order if the telephone company feels the order is too burdensome.

(12) The SAC's approval of a Form 9170, Request for Pen Register and/or Trap and Trace Devices, is required to obtain authorization to use trap and trace devices. After SAC approval, the Form 9170 must be electronically forwarded to Special Investigative Techniques.

9.4.6.7.5 (07-03-2013) **Use and Approval of Electronic Tracking Devices**

(1) When the use of an electronic tracking device is necessary during an investigation that CI has the authority to investigate, special agents are required to obtain a search warrant, following the general search warrant procedures set forth in IRM 9.4.9, Search Warrants, Evidence and Chain of Custody (see subsections 9.4.9.2, General Search Warrant Procedures and 9.4.9.3, Search Warrant Process).

(2) Electronic tracking and global positioning system search warrants are authorized under a primary investigation (PI).

(3) There is a forty-five (45) day time limit for electronic and GPS tracking (subject to extensions for good cause), the search warrant affidavit should clearly indicate the period of time necessary for electronic tracking and monitoring. This time frame should include the time necessary for maintaining the equipment. Potential and future extensions should be taken into consideration when determining the period for tracking and monitoring.

(4) In keeping with IRM 9.4.9 (subsection 9.4.9.2), electronic tracking search warrant affidavits require evaluation by Criminal Tax (CT) Counsel. The search affidavit should include the following:

a. investigative need for tracking and monitoring of information
b. identification of vehicles upon which the device will be attached
c. potential locations of the vehicles when the device will be attached
d. period of time necessary for monitoring
e. equipment installers and users
f. authorization to perform necessary maintenance to the device (e.g., battery replacement) and removal of the device

(5) In situations involving sensitive targets, IRM 9.4.9 (subsection 9.4.9.3.3.3, Department of Justice, Tax Division Approval) also applies.

(6) Non-CI affiant tracking search warrants requiring CI special agents participation by attaching, monitoring, maintaining or removing the tracking device, requires adherence to IRM 9.4.9 (subsection 9.4.9.3.4, Non-IRS-Criminal Investigation Affiant Search Warrants).

9.4.6.8
(07-03-2013)
Internet-Related Investigative Activities

(1) The Internet provides a wealth of information that may be relevant to CI investigations because it has become a widely used means to communicate and to conduct business. Records of Internet transactions may also be important evidence to investigators. As a general rule, the same policies and procedures that govern investigations in the physical world apply to investigations in cyberspace. Agents should therefore apply the most analogous real-world rules and procedures to each online investigative technique they seek to use. For example, law enforcement officials may obtain information from publicly accessible online sources and facilities (web sites, listservs, news groups, chat rooms, etc) under the same conditions they may obtain information from other sources generally open to the public (e.g., newspapers, libraries, etc.). Similarly, the same policies, procedures, and restrictions that apply to physical world investigative activities (for example, restrictions on access to private places, agent identification, and undercover activities) apply equally to online investigative activities. Agents are authorized to conduct surveillance activities on internet social networking, including Facebook, Twitter, Google+, etc., under the following conditions:

a. A special agent may assume a temporary pretext identity, (IRM 9.4.8, Undercover Operations (subsection 9.4.8.1(4)), when accessing social networking web sites for surveillance purposes only.
b. Communication, of any kind, between a target, associate, or any other individual, through internet social networking sites utilizing a pretext identity requires an approved undercover operation. Communication includes, but is not limited to, “friend” requests, instant messaging, posts on message boards, etc.
c. c) Surveillance of social networking web sites may only be conducted under an approved General, Primary or Subject Investigation. Surveillance of social networking web sites may be conducted by any special agent since communication is prohibited under this section.
d. d) Internet surveillance may only be conducted on a non-CI networked, undercover computer. Computers which leave no government footprint are required for use in this type of surveillance.
e. e) The SAC will be responsible for monitoring internet surveillance and ensuring proper procedures are followed.

(2) Special rules apply to the interception of online communications and the gathering of information kept by online service providers (see subsections 9.4.6.7.2; 9.4.6.7.3; and 9.4.6.7.4).

(3) Special agents should consult with the CIS in the local field office, the Electronic Crimes Program in HQ, or the Computer and Telecommunications Coordinator in the local US Attorney's office for advice on conducting online investigations or with questions on using the internet for investigative purposes.

(4) The CIS of the Electronic Crimes Program can also provide technical support in the use of techniques, tools, and non-CI network computer equipment needed to conduct many online investigative activities.

9.4.6.9
(09-05-2008)
Video Surveillance

(1) The wiretap statute does not prohibit the use of video equipment to record or monitor a public meeting. Any attempt to acquire the participants' conversations by the video equipment or with other devices, however, must be done in accordance with the provisions of the wiretap statute. The local Criminal Tax attorney should be consulted for advice on the application of the wiretap statute.

(2) A journeyman level special agent has authority to conduct video surveillance.

(3) A search warrant pursuant to 18 USC §3102 and Rule 41(a) of the Federal Rules of Criminal Procedure (Fed. R. Crim. P.) is required to obtain evidence that cannot be observed from a public place with the un-aided eye. If video surveillance from a place not accessible to the public, or if sense enhancing technology is contemplated, the local Criminal Tax attorney should be consulted prior to using this technique.

9.4.6.9.1
(07-03-2013)
Video Surveillance of Public View Areas

(1) Use of a video camera or IP camera (pole cameras) to observe activity that is viewable by the public (either because members of the public can lawfully access the area where this activity occurs or can see the activity from a lawful vantage point) does not generally constitute an intrusion into a constitutionally protected private interest. A warrant is generally not required to visually record activities that occur in publicly accessible areas such as public parks, sidewalks, streets, open fields, and other areas outside the curtilage of a house that is not commonly accessible to the public.

(2) The Fourth Amendment does not require law enforcement officers to shield their eyes when passing a home on a public thoroughfare. Officers may, without a search warrant, use video surveillance to assist them in observing certain areas even when the areas are within the curtilage of a house if others can observe these same areas from a place they are lawfully entitled to be (i.e., from the street, sidewalk, or an open field). This would include unobstructed video surveillance of driveways, front doorways, and yards of businesses or houses.

(3) Special rules apply to the video surveillance of the workplace. In general, video surveillance of an area of the workplace that is accessible and viewable by others during work hours may be done without a search warrant. Video surveillance of employee work areas that are not publicly accessible or viewable usually may not be undertaken without a search warrant. The local Criminal Tax attorney should be consulted when there is any question whether a particular area is publicly accessible.

(4) Special Agent in Charge approval is required when:

a. The installation of video or IP cameras requires the use of an outside utility company for the power drop.
b. The camera installation, or its use, will incur expenses that must be paid by the field office.

(5) Approval should be obtained using the "Video Surveillance Memorandum" in Document Manager. The request should include a summary of the investigation, the reason other surveillance techniques will not work, and expenses associated with the installation.

9.4.6.9.2
(09-05-2008)
Public Access and Other Areas Entitled to Fourth Amendment Protection

(1) Video surveillance into public areas, e.g., a rest room, where one would reasonably expect his/her actions to be private, must comply with Fourth Amendment standards and may require a warrant.

9.4.6.9.3
(09-24-2003)
Video Surveillance When Consenting Party is Present

(1) Special agents may also observe and record (video) private meetings between undercover officer(s) or cooperating witness(es) and subjects if the premises are controlled by the special agent or witness.

9.4.6.10
(09-05-2008)
Aerial Surveillance

(1) Aerial surveillance is not subject to the wiretap statute and is generally not considered to constitute a search within the meaning of the Fourth Amendment.

(2) Supreme Court rulings are based on whether or not a person has a constitutionally protected reasonable expectation of privacy. This involves:

a. whether the person had an actual exception of privacy
b. whether society recognizes that expectation as being reasonable

(3) The Supreme Court has held an individual taking measures to restrict views of his activities does not preclude an officer's observation from a public vantage point where he/she has a right to be and which renders the activities clearly visible. In these cases, the police observations takes place within public navigable airspace, in a physically non-intrusive manner, and any member of the flying public in the airspace who cared to glance down could have made the same observations. The Fourth Amendment does not require a search warrant in order to observe what is visible to the un-aided eye. If, however, some enhancement device is used during the overflight, the general rule may not apply.

(4) The SAC will approve, in writing, the use of aerial surveillance. The request must include a summary of the investigation, the reason why other surveillance techniques will not work, the budget issues, and the minimum requirements of the pilot/crew.

9.4.6.10.1
(09-05-2008)
Use of Aircraft

(1) An aircraft may be used in investigative situations such as:

a. surveillance
b. electronic tracking
c. communications relay
d. aerial photography
e. undercover support
f. expeditious transport of special agents or equipment in emergency situations

(2) Federal, state, and local government aircraft should be used where available. When not available, aircraft may be rented or leased from a local aviation service. When a decision is made to rent or lease an aircraft, the following procedures should be used:

a. prepare and forward a requisition to the appropriate payment office; or
b. establish an imprest fund in support of the operation

(3) To pilot an aircraft, special agents must meet the following minimum standards:

a. 500 hours flight time
b. 100 hours cross-country flight time
c. 100 hours of actual or simulated instrument flight time
d. FAA Commercial Pilot certificate (appropriate category)
e. current FAA instrument ratings
f. current FAA Second-Class Medical certificate

(4) The minimum crew for aircraft surveillance will be a pilot and an observer. Except for the pilot, only special agents or other Federal, state, or local law enforcement agents or officers will conduct surveillance.

(5) All aircraft will be operated under Federal Aviation Administration (FAA) certification and Federal Aviation Regulations. Aircraft will be flown in accordance with the applicable flight manuals and performance limitations. Any deviation shall be approved in advance by the local FAA office. Aircraft accidents or incidents shall be reported to the National Transportation Safety Board (NTSB) in accordance with NTSB Regulations.

9.4.6.11
(09-24-2003)
Report of Electronic Surveillance Information Received From State or Local Agencies

(1) The SAC will submit a report through proper channels, including the Director, Field Operations to the Chief, CI, concerning electronic surveillance information received from state or local agencies. The report must be submitted within 30 days after the information is received.

(2) The report of electronic surveillance information received from a state or local agency shall contain the following information:

a. the investigation name and number (if applicable)
b. the names of the persons whose conversations were monitored, if applicable
c. a summary of the information obtained, including the names of all individuals mentioned in the monitored conversations
d. the locations (address) where any monitored conversations took place and, if applicable, the telephone number of the telephone on which the monitoring equipment was installed
e. the name of the agency that conducted the electronic surveillance
f. the periods of time that the equipment was used (dates and times)

g. the name of the IRS employee who has custody of the records relating to the monitoring, or the name and location of the IRS activity to which the information was transmitted

Exhibit 9.4.6-1 (09-24-2003)
2703(d) Order

Sample 18 U.S. C. § 2703(d)
Application and Order

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN RE APPLICATION OF	)	
THE UNITED STATES OF AMERICA FOR	)	MISC. NO. _____
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(D)	)	**Filed Under Seal**

APPLICATION [Name], an Assistant United States Attorney for the _____ District of _____, hereby files under seal this ex-parte application for an Order pursuant to 18 U.S.C. Section 2703(d) to require [Internet Service Provider], [mailing address], to provide records and other information pertaining to the [Internet Service Provider] network account that was assigned Internet Protocol address [xxx.xxx.xxx.xxx] on [date] and [time].

The records and other information requested are set forth as Attachment 1 to the Application and to the proposed Order. In support of this Application, the United States offers the following:

FACTUAL BACKGROUND

1. The United States Government, including the Internal Revenue Criminal Investigation and the Department of Justice, are investigating *[brief description of type of case and how computers are being utilized*]. Investigation to date of these incidents provides reasonable grounds to believe that [Internet Service Provider] has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation.

Cite the specific and articulate facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

LEGAL BACKGROUND

2. 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information in the possession of providers of "electronic communications services" and/or "remote computing services." [Internet Service Provider] functions both as an electronic communications service provider -- that is, it provides its subscribers access to electronic communication services, including e-mail and the Internet -- AND/OR a remote computing service (provides computer facilities for the storage and processing of electronic communications) -- as those terms are used in 18 U.S.C. § 2703. **[Note that because**

Exhibit 9.4.6-1 (Cont. 1) (09-24-2003)
2703(d) Order

a "remote computing service" is public by definition, this statement must be modified if you are seeking information from a service provider who is not a provider to the public, such as, for example, a university.]

3. Here, the government seeks to obtain three categories of records: (1) basic subscriber information; (2) records and other information, including connection logs, pertaining to certain subscribers; and **[Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b) as opposed to mere records pursuant to § 2703(c).]** (3) the content of electronic communications in a remote computing service (but not communications in electronic storage).

4. To obtain basic subscriber information, such as the subscriber's name, address, length and type of service, connection and session records, telephone or instrument number including any temporarily assigned network address, billing information, and other identifying records, the government needs only a subpoena; however, the government may also compel such information through an Order issued pursuant to section 2703(d). See 18 U.S.C. § 2703(c)(1)(B), (c)(2). To obtain other types of records and information pertaining to the subscribers or customers of service providers, including connection logs and other audit information, the government must comply with the dictates of sections 2703(c)(1)(B) and 2703(d). Section § 2703(c)(1)(B) provides in pertinent part:

   A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the governmental entity … obtains a court Order for such disclosure under subsection (d) of this section;

5. **[Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).]** To obtain the contents of electronic communications held by a remote computing service (but not the contents in "electronic storage," see n.1), the government must comply with 2703(b)(1)(B), which provides, in pertinent part:

   > A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph 2 of this subsection … with prior notice from the government entity to the subscriber or customer if the governmental entity… obtains a court Order for such disclosure under subsection (d) of this section .. except that delayed notice may be given pursuant to section 2705 of this title.
   >
   > Paragraph 2 of subsection 2703(b) applies with respect to any electronic communication that is held or maintained on a remote computing service-
   >
   > (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

Exhibit 9.4.6-1 (Cont. 2) (09-24-2003)
2703(d) Order

> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Therefore, communications described in paragraph 2 of subsection 2703(b) include the content of electronic mail that has been opened, viewed, downloaded, or otherwise accessed by the recipient and is held remotely by the service provider on its computers.

6. All of the information the government seeks from [Internet Service Provider] through this application may be compelled through an Order that complies with section 2703(d). Section 2703(d) provides in part:

> A court Order for disclosure under subsection ... (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the ... records or other information sought, are relevant and material to an ongoing criminal investigation ... A court issuing an Order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such Order, if the information or records requested are unusually voluminous in nature or compliance with such Order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth specific and articulable facts showing there are reasonable grounds to believe that the materials sought are relevant and material to the ongoing criminal investigation.

GOVERNMENT'S REQUEST

7. The government requests that the [Internet Service Provider] be directed to produce all records described in Attachment 1 to this Application. This information is directly relevant to identifying the individual(s) responsible for the crime under investigation. The information requested should be readily accessible to [Internet Service Provider] by computer search, and its production should not prove to be unduly burdensome. **[undersigned should check with the ISP before filing this document to ensure the accuracy of this statement.]**

8. The United States requests that this Application and Order be sealed by the Court until such time as the court directs otherwise.

9. The United States further requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), that [Internet Service Provider] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this Order for such period as the court deems appropriate. The United States submits that such an Order is justified because notification of the existence of this Order could seriously jeopardize the ongoing investigation. Such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

Exhibit 9.4.6-1 (Cont. 3) (09-24-2003)
2703(d) Order

10. **[Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b) as opposed to mere records pursuant to § 7203(c):]** The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an Order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of 90 days. Providing prior notice to the subscriber or customer could seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee, or continue this flight from prosecution.

[*Additional Baker Act language to use if the ISP is a university:* The United States further requests that [Internet Service Provider]'s compliance with the delayed notification provisions of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(J)(ii) (the "Baker Act"). See 34 CFR § 99.31 (a)(9)(i) (exempting requirement of prior notice for disclosure made to comply with a judicial Order or lawfully issued subpoena where the disclosure is made pursuant to "any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed")].

WHEREFORE, it is respectfully requested that the Court grant the attached Order, (1) directing [Internet Service Provider] to provide the United States with the records and information described in Attachment 1; (2) directing that the Application and Order be sealed; (3) directing [Internet Service Provider] not disclose the existence or content of the Order, except to the extent necessary to carry out the Orders; and **[use only if the application seeks to obtain the contents of communication pursuant to § 2703(b)]** and (4) directing that the notification by the government otherwise required by 18 U.S.C. § 2703(b) be delayed for ninety days.

Respectfully submitted,

_____
Assistant United States Attorney

Exhibit 9.4.6-1 (Cont. 4) (09-24-2003)
2703(d) Order

ATTACHMENT A

You are to provide the following information as printouts and as ASCII data files (or describe media on which you want to receive the information sought), if available:

1. The following customer or subscriber account information for any accounts registered to [subscriber], or associated with [subscriber]. For each such account, the information shall include:

   a) name(s) and email address;
   b) address(es);
   c) local and long distance telephone connection records, or records of session times and durations;
   d) length of service (including start date) and types of service utilized;
   e) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
   f) the means and source of payment for such service (including any credit card or bank account number).

2. User connection logs for:

   a) all accounts identified in Part A, above,
   b) the IP address [list IP address, e.g. 999.999.999.999],

for the time period beginning [date] through and including the date of this Order, for any connections to or from [provider or service].

User connection logs should contain the following:

   1. Connection time and date;
   2. Disconnect time and date;
   3. Method of connection to system (e.g., SLIP, PPP, Shell);
   4. Data transfer volume (e.g., bytes);
   5. Connection information for other systems to which user connected via [provider or service], including:
      a. Connection destination;
      b. Connection time and date;
      c. Disconnect time and date;
      d. Method of connection to system (e.g., telnet, ftp, http);
      e. Data transfer volume (e.g., bytes);
      f. Any other relevant routing information.

3. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **The contents of electronic communications (not in electronic storage[3]) that were placed or stored in [provider or service]'s computer systems in directories or files owned or controlled by the accounts identified in Part A at any time after [date of earliest intrusion] up through and including the date of this Order.**

Exhibit 9.4.6-1 (Cont. 5) (09-24-2003)
2703(d) Order

UNITED STATES DISTRICT COURT
FOR THE_____ DISTRICT OF _____

IN RE APPLICATION OF THE	)
UNITED STATES OF AMERICA FOR	) MISC. NO. _____
AN ORDER PURSUANT TO	)
18 U.S.C. § 2703(d)	) Filed Under Seal

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(b) and (c), which application requests the issuance of an Order under Title 18, United States Code, Section 2703(d) directing [Internet Service Provider], an electronic communications service provider and a remote computing service, located in the _____ District of _____, to disclose certain records and other information, as set forth in Attachment A to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **and the contents of electronic communication** sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and Order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that [Internet Service Provider] will, within three days of the date of this Order, turn over to agents of the Internal Revenue Service, Criminal Investigation the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this Application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that [provider or service] shall not disclose the existence of the Application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court. [Optional Buckley Amendment language: Accordingly, [Internet Service Provider]'s compliance with the non-disclosure provision of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(j)(ii).]

Exhibit 9.4.6-1 (Cont. 6) (09-24-2003)
2703(d) Order

[Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. 2703(b)(1)(B) be delayed for a period of [ninety days].**

_____
United States Magistrate Judge

_____
Date

Exhibit 9.4.6-2 (09-03-2020)
Reserved

Sample Language for Preservation Request Letters under 18 U.S.C. § 2703(f)

[Internet Service Provider]
[Address]
VIA FAX to (xxx) xxx-xxxx

Dear Mr. [ ]:

I am writing to confirm our telephone conversation earlier today and to make a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record. You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. **If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions.**

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

[In a case involving an e-mail account]

A. All stored electronic communications and other files reflecting communications to or from the following electronic mail address: **[JDoe@isp.com];**

B. All records and other evidence relating to the subscriber(s), customer(s) account holder(s), or other entity(ies) associated with the e-mail address **[JDoe@isp.com]** or user name **"Jdoe,"** including, without limitation, subscriber names, user names, screen names, or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and

C. Any other records and other evidence relating to the e-mail address **[JDoe @isp.com]** or user name **"Jdoe."** Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with user activity or relating to communications and any other activities to, through or from **[JDoe@isp.com]** or user name **"Jdoe,"** whether such records or other evidence are in electronic or other form.

Exhibit 9.4.6-2 (Cont. 1) (09-03-2020)
Reserved

[In a case involving use of a specific I.P. address]

All electronic records and other evidence relating to the use of the IP address 222.222.22.2 or domain name abc.wcom.net on September 5, 1999 at 4:28 and 04:32 GMT + 02:00, and on September 7, 1999 at 00:19 GMT + 02:00.

[In a case involving activity of a user account]

All connection logs and records of user activity for the user name **Jdoe** or address **[Jdoe@isp.com],** including:

1. Connection date and time;
2. Disconnect date and time;
3. Method of connection (e.g. telnet, ftp, http);
4. Data transfer volume;
5. User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
6. Telephone caller identification records; and
7. Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with **[JDoe@isp.com]**, including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.

Any other records and other evidence relating to **[JDoe@isp.com]**. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through **[JDoe@isp.com]**, whether such records or other evidence are in electronic or other form.

(Although this request does not apply to the preservation of voicemail or other actual stored oral communications, any other records, data, or connection logs pertaining to such stored oral communications are to be preserved.)

If you have any questions or need assistance, please contact me at (xxx) xxx-xxxx.

Sincerely,

(Name)
Supervisory Special Agent

Exhibit 9.4.6-3 (09-24-2003)
Application for Pen Register

Application – Trap and Trace
Pen Register
Form 13

UNITED STATES DISTRICT COURT
_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE OF A)
(TRAP AND TRACE DEVICE))
(PEN REGISTER))
_____)

APPLICATION

_____, an attorney of the United States Department of Justice, being duly sworn, hereby applies to the Court for an order authorizing the installation and use of a (trap and trace device) (pen register) on telephone number(s) _____. In support of this application I state the following:

1. Applicant is an "attorney for the Government" as defined Rule 54(c) of the Federal Rules of Criminal Procedure, and, therefore, pursuant to Section 3122 of Title 18, United States Code

100a

Exhibit 9.4.6-3 (Cont. 1) (09-24-2003)
Application for Pen Register

may apply for an order authorizing the installation and use of a (trap and trace device) (pen register).

2. Applicant certifies that the (investigative agency) is conducting a criminal investigation of (name targets) and others as yet unknown, in connection with possible violations of (list violations); it is believed that the subjects of the investigation are using telephone number (s) _____, (listed in the name of) (leased to) _____ and located at _____ in furtherance of the subject offense; and that the information likely to be obtained from the (trap and trace device) (pen register) is relevant to the ongoing criminal investigation in that it is believed that this information will concern the aforementioned offenses.

3. Applicant requests that the Court issue an order authorizing the installation and use of a (trap and trace) (pen register) device to capture the (incoming) (outgoing) electronic or other impulses which identify the (originating) (outgoing) number of a wire or electronic communication and the date, time and duration of such (incoming) (outgoing) impulses for a period of (time period, not to exceed 60) days.

101a

Exhibit 9.4.6-3 (Cont. 2) (09-24-2003)
Application for Pen Register

4. The applicant requests further that the order direct that the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the (trap and trace device) (pen register), including installation and operation of the device(s), occur unobtrusively and with a minimum of disruption of normal telephone service. The communications service provider shall be compensated by the applicant for reasonable expenses incurred in providing such facilities and technical assistance.

5. The applicant requests further that the order direct that the results of the (trap and trace device) (pen register) shall be furnished to Special Agents of the (investigative agency) at reasonable intervals during regular business hours for the duration of the order.

6. The applicant requests further that the Court's order direct (communications service provider), and its agents and employees not to disclose to the subscriber, or any other person, the existence of this order, the (trap and trace device) (pen register), of this investigation unless or until otherwise ordered by the Court.

102a

Exhibit 9.4.6-3 (Cont. 3) (09-24-2003)
Application for Pen Register

(in the case of a trap and trace)

7. The applicant further requests that the Court's order be limited in the following respects:

(a) the tracing operation shall be limited to (Electronic Switching System (ESS)) or (No. 5 cross-bar switching facilities); and

(b) the tracing operation shall be restricted to tracing and recording only those incoming calls originating from (geographical area).

WHEREFORE, it is respectfully requested that the Court grant an order for (enter time period, not to exceed 60) days (1) authorizing the installation and use of a (trap and trace device) (pen register) to identify (incoming) (outgoing) calls on telephone number (s) _____, (2) directing the (communications service provider) to forthwith furnish agents of the (investigative agency) with all information, facilities and technical assistance necessary to accomplish the installation of the (trap and trace device) (pen register), including installation and operation of the device (s), unobtrusively and with minimum

103a

Exhibit 9.4.6-3 (Cont. 4) (09-24-2003)
Application for Pen Register

Interference to the service presently accorded the person (s) whose telephone (s) is to be the subject of the device (s), (3) directing the (service provider) and its agents and employees not disclose to the subscriber or any other person the existence of the Court's order, (trap and trace device) (pen register) or this investigation unless or until otherwise ordered by the Court, and (4) sealing the application and the Court's order.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on _____, 19 _____

_____

Applicant

104a

Exhibit 9.4.6-4 (09-24-2003)
Court Order for Pen Register

Order – Trap and Trace
Pen Register
Form 14

UNITED STATES DISTRICT COURT
_____DISTRICT OF_____

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR AN ORDER AUTHORIZING)
THE INSTALLATION AND USE OF A)
(TRAP AND TRACE DEVICE))
(PEN REGISTER))
_____)

ORDER

This matter having come before the Court pursuant to an application under oath pursuant to Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which requests an order under Title 18, United States Code, Section 3123, authorizing the installation and use of a (trap and trace device) (pen register) on telephone number(s) _____, the Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of (list violations) by (list targets) and others as yet unknown.

IT APPEARING that the information likely to be obtained by a (trap and trace device) (pen register) installed on telephone number(s) _____, (subscribed to) (leased by)

105a

Exhibit 9.4.6-4 (Cont. 1) (09-24-2003)
Court Order for Pen Register

_____, and located at _____, is relevant to an ongoing criminal investigation of the specified offenses,

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of (investigative agency) may direct (communications service provider) to install a (trap and trace device) (pen register) on telephone number (s) _____ to capture the (incoming) (outgoing) electronic or other impulses which identify the originating (outgoing) number of a wire or electronic communication and the date, time, and duration of such (incoming) (outgoing) impulses for a period of (enter time period, not to exceed 60) days; and

IT IS ORDERED FURTHER, pursuant to Title 18, United States Code, Section 3123 (b) (2), that (communications service provider) shall furnish agents of the (investigative agency) forthwith all information, facilities and technical assistance necessary to accomplish the installation of the (trap and trace device) (pen register), including installation and operation of the device(s), unobtrusively and with minimum interference to the services that are accorded persons whose

106a

Exhibit 9.4.6-4 (Cont. 2) (09-24-2003)
Court Order for Pen Register

telephone (s) is/are to be the subject of the device (s).

IT IS ORDERED FURTHER that the (investigative agency) will compensate the (communication service provider) for expenses reasonably incurred in complying with this order.

IT IS ORDERED FURTHER that the results of the (trap and trace device) (pen register) shall be furnished to the (investigative agency) at reasonable intervals during regular business hours for the duration of the order.

(in the case of a trap and trace)

IT IS ORDERED FURTHER that: a) the tracing operation shall be limited to (Electronic Switching System (ESS) or (No.5 cross-bar switching facilities); and b) the tracing operation shall be restricted to tracing and recording only those incoming calls originating from (geographical area).

IT IS ORDERED FURTHER, pursuant to Title 18, United States Code, Section 3123 (d), that this order and the application be sealed until otherwise

107a

Exhibit 9.4.6-4 (Cont. 3) (09-24-2003)
Court Order for Pen Register

ordered by the Court, and that (communications service provider), its agents and employees shall not disclose the existence of the (trap and trace device) (pen register), the existence of this order, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the Court.

_____

UNITED STATES DISTRICT JUDGE

_____

Date

108a