PURPOSE

(1) This transmits revised IRM 9.4.9, Investigative Techniques, Search Warrants, Evidence, and Chain of Custody.

MATERIAL CHANGES

(1) Pursuant to Fed. R. Crim. P. Rule 41 (e) (2), subsections 9.4.9.3.1.4 and 9.4.9.3.6 are revised to state that the Magistrate Judge reviews and signs search warrants. The warrant commands the officer/special agent to: "(i) execute the warrant within a specified time no longer than 14 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant, including a copy of the inventory, to the magistrate judge designated in the warrant."

(2) Subsection 9.4.9.3.2 paragraph (3) is added to clearly outline the role of the Tax Fraud Investigative Aide (TFIA) in the planning and preparation of enforcement actions. To further clarify the TFIA's role, IRM 9.4.11 is also updated to state that the TFIA's role must be clearly defined in the Plan of Action and Risk Assessment Guide.

(3) Former subsection 9.4.9.3.2 paragraphs (3) through (5) are renumbered consecutively.

(4) Subsection 9.4.9.3.3.3 paragraph (3) is revised to state that the Special Agent in Charge must advise the Director, Field Operations before referring search warrant documents to the Department of Justice, Tax Division. Director, Field Operations concurrence is not required.

(5) Subsection 9.4.9.4 paragraphs (1) and (3) are revised to state that in addition to the documents maintained in the group files, a copy of the Enforcement Action Review Form must be maintained in the Special Agent in Charge's administrative files.

(6) This manual update is approved pursuant to the January 14, 2010, Change in Time to Execute a Warrant memorandum and the March 18, 2009, TFIA Participation in Search Warrants memorandum.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 9.4.9 dated August 2, 2010. This IRM also incorporates procedure(s) implemented by the following: Director, Warrants & Forfeitures' memorandum dated January 14, 2010, [Subject: "Change in Time To Execute a Warrant"] and Director, Operations Policy and Support's memorandum dated March 18, 2009, [Subject: "TFIA Participation in Search Warrants"].

AUDIENCE

CI

EFFECTIVE DATE

(03-17-2011)

Terry L. Stuart for Victor S O Song
Chief, Criminal Investigation

9.4.9
Search Warrants, Evidence and Chain of Custody

Table of Contents

9.4.9.1
(10-05-2007)
Overview

(1) This section discusses agency policy and procedural requirements for use of search warrants by Criminal Investigation (CI) special agents. It includes guidelines regarding the execution of the search warrant and the seizure of evidence, computers, and contraband. Further, it sets forth the proper procedures for maintaining the chain of custody and transferring evidence to the forensic lab.

(2) Special agents should be aware that not every investigation requires the execution of a search warrant. Form 6884, Voluntary Consent to a Search of Person, Premises or Conveyance, (see Document Manager), is an effective tool for obtaining investigative evidence. Special agents should discuss with their Supervisory Special Agent (SSA) the benefits and risks of confronting the individual in possession of the evidence sought as opposed to executing a search warrant.

9.4.9.2
(06-19-2008)
General Search Warrant Procedures

(1) A numbered subject criminal investigation (SCI) is required when CI is the affiant for a search warrant. The Criminal Investigation Management Information System (CIMIS) must be updated to reflect search warrant activity for **CI affiant and non-CI affiant search warrants**.

(2) Special agents need either a numbered primary investigation (PI) or SCI to participate in the execution of non-CI affiant search warrants. Please refer to IRM 9.9.4 for additional information.

(3) Search warrants for tax and tax-related offenses will be utilized with restraint and only in significant tax investigations. All other investigative tools (i.e., mail covers, surveillance, informants, trash pulls) should be considered before deciding that a search warrant is the least intrusive means to acquire the evidence. The significance of a tax investigation can be evaluated by considering the following:

- amount of tax due
- nature of the fraud
- need for evidence to be seized
- impact of the potential criminal tax investigation on voluntary compliance

(4) All requests for tax and tax-related search warrants will require a written evaluation by Criminal Tax (CT) Counsel of the intrusiveness issue. Internal Revenue Manual (IRM) 9.1.4, Criminal Investigation Directives (Directive No. 1) is interpreted to mean that CI special agents will employ the least intrusive means necessary to acquire evidence in tax and tax-related Title 18 investigations.

Note: In this context, tax-related investigations are those that must be authorized by the Department of Justice (DOJ), Tax Division. Typically, these investigations involve violations of 18 USC §286, 18 USC §287, and 18 USC §371.

(5) In addressing intrusiveness, the special agent will explain in Form 13739, Enforcement Action Review Form (EARF) (see Document Manager) why other investigative methods cannot produce the evidence being sought, and why the search warrant represents the best and least intrusive method to secure the evidence. Some factors that will be considered by management and CT Counsel in evaluating the intrusiveness issue are:

- type of records sought
- any objective evidence indicating the subject may destroy the evidence

- any objective evidence of the subject's attempt to obstruct the investigation
- facts that establish that other attempts to acquire the records were ineffective
- facts that indicate that other methods of acquiring the records may compromise the investigation

9.4.9.3
(02-09-2005)
Search Warrant Process

(1) A search warrant can be an effective investigative tool once it has been determined that crucial evidence of a particular crime exists, is likely to be found at a specific location, and cannot be obtained by any other means. There are five major steps to the process:

a. preparing the search warrant application
b. planning the enforcement action
c. obtaining approval
d. executing the search warrant and preserving the evidence
e. adhering to the applicable post operation procedures

(2) It is the special agent's responsibility to proof all documents prepared by the attorney for the government. The search warrant is returned by the court giving the special agent the legal authority to execute the warrant at the particular place and time, and to seize the specific items or person(s) described. It is imperative that the special agent review the prepared search warrant to ensure all the proper information from the Application and Affidavit for Search Warrant is contained in the search warrant issued by the court. The warrant must be sufficient on its face or refer to an affidavit that is sufficiently incorporated therein, and specifically set forth:

- the violations being investigated
- a description of the person/premises to be searched
- a description of the items to be seized

Note: The Supreme Court, in *Groh v. Ramirez, 124 S. Ct. 1284* (February 24, 2004), ruled a search warrant that failed to describe the persons or things to be seized was invalid on its face, notwithstanding that the requisite particularized description was provided in the unincorporated search warrant application. The court also ruled that the Federal agent who had prepared the search warrant and supervised its execution was not entitled to qualified immunity from liability. This decision, along with the Ninth Circuit's recent decision in *United States v. Bridges, 344 F.3d 1010* (9th Cir. 2003), clearly highlights the need for a warrant to contain on its face or in an incorporated and attached search warrant application, sufficient information to instruct both the executing officer and the occupant of the place to be searched of the nature of the alleged violation(s) and the description of the items to be seized.

9.4.9.3.1
(10-05-2007)
Preparing the Search Warrant Documents

(1) A search warrant consists of a set of documents, each with a specified legal purpose. These documents are:

a. Application for Search Warrant
b. Affidavit
c. Search Warrant
d. Search Warrant Attachment "A" description of "Location to be searched"
e. Search Warrant Attachment "B" description of "Items to be seized"
f. Search Warrant Return

9.4.9.3.1.1
(10-05-2007)
Application and Affidavit for Search Warrant

(1) The Affidavit for Search Warrant, (see Document Manager), is a standard form signed and sworn by the special agent that summarizes the specifics of the search warrant. The application addresses the particulars of the person, property, or premises to be searched; the title and employing agency of the special agent; the judicial district where the person or property exists; a description of the items to be seized; and the nature of the alleged criminal violations. This section of the form is generally prepared by the attorney for the government assigned to the investigation.

(2) In order to obtain a search warrant, the special agent must convince internal and external approving officials, and ultimately a Federal Judge Magistrate (magistrate), that there is probable cause to believe that:

a. A crime has been committed.
b. Items sought may be seized by virtue of their connection to the crime.
c. Items sought are on the premises to be searched.

(3) The remainder of the application is the affidavit in support of the application drafted by the special agent along with input from CT Counsel and, if it is a grand jury investigation, the attorney for the government.

9.4.9.3.1.2
(10-05-2007)
Affidavit

(1) The affidavit sets forth, in a logical fashion, all the existing evidence to establish probable cause that a crime was committed, that evidence of the crime exists, and that the evidence is located at a particular location.

(2) A suggested format for the affidavit includes the following sections:

a. affiant's training, experience, and expertise
b. detailed account of the criminal statutes that are alleged to have been violated and evidence to show probable cause that the statutes have been violated
c. financial evidence
d. description of the place to be searched and nexus between the location to be searched and the subject of the investigation
e. conclusions which tie evidence to the violations, the subject, the location and the time period

(3) Any time a special agent believes that evidence may be contained on a computer, a Computer Investigative Specialist (CIS) will be consulted at the initiation of the discussions in anticipation of a search warrant. The CIS will assist the special agent in drafting the search warrant affidavit and the list of items to be seized. As needed, the CIS will also assist in the interview of key witnesses/informants who have knowledge of the computers. Specific information must be developed regarding the subject's use of the computer and the role of the computer(s) in the offense.

a. The special agent and CIS will develop probable cause for evidence contained in computers and for each component of the computer. The special agent must articulate a factual basis to believe that the computer was used for the creation and/or storage of evidentiary records and, if necessary, explain in the affidavit why an on-site search is not reasonable. He/she will then request permission to seize the computer and search it later.
b. In contemplating the seizure of computers, special agents must be aware of the possibility that protected material may be stored in the computer. A positive statement must be included in the search warrant that no work

product material exists on the computer. If protected material exists on the computer, state how the material is going to remain protected. Magistrates can authorize a segregation plan; address the possibility of e-mail on the computer; indicate the e-mail status in the search warrant affidavit and the search warrant itself; identify in the search warrant whose e-mail is going to be read; and determine whether such e-mail is subject to a search. (See 18 USC §2703.)

c. The special agent will consult with CT Counsel and/or the attorney for the government on computer issues during the investigation. Computer and Telecommunications Coordinators (CTCs) at the local US Attorney or Assistant US Attorney's (AUSA) office who have received special training in the computer crimes subject area are available at: Tax Division, DOJ: Senior Trial Attorney, (202) 514-2832 and Fax (202) 514-3081 and/or Computer Crime and Intellectual Property Section, DOJ at (202) 514-1026 and fax (202) 514-6113.

(4) Unlike a criminal trial, the rules of evidence do not apply to a search warrant application and all evidence, whether direct, indirect, hearsay, or based upon personal knowledge, can be included in the affidavit to establish probable cause. Only that evidence which is necessary to establish probable cause need be disclosed in the affidavit. Consideration should therefore be given to the amount of investigative disclosure contained in the affidavit should it be unsealed before the conclusion of the investigation.

(5) The use of hearsay information (i.e., information which was not obtained through direct personal knowledge and which is normally inadmissible in a criminal trial proceeding) may be included in the affidavit. It is common for an affidavit to contain the investigative findings of other police officers, Federal agents, independent third parties, etc.

(6) Hearsay and other information provided by an informant is subject to a higher degree of scrutiny. Three landmark Supreme Court cases, **Aquilar, Spinelli, and Gates**, frame much of the current procedures involving the use of informant testimony. **Aquilar** and **Spinelli** established a two-prong test that has to be satisfied in order to use information from a particular informant. This test required that both the reliability and veracity (credibility) of an informant be established in order to use any information from the informant. The **Gates** decision modified **Aquiler** and **Spinelli**, holding that it is not necessary to apply the two prongs of the test independent of each other; rather, the credibility of the information provided by an informant may be evaluated in light of everything that is known at that point in the investigation. This standard is known as the " totality of the circumstances" and the **Gates** decision states: "The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that either contraband or evidence of a crime will be found in a particular place. And the duty of a reviewing court is simply to ensure that the magistrate had a 'substantial basis for ….conclude[ing]' that probable cause [462 US 213, 239] existed."

(7) The reliability of an informant can be established by the following:

- informant has a history of providing accurate information
- information from the informant has been independently corroborated
- informant has a satisfactory history as an informant with other law enforcement agencies

(8) The veracity or credibility of the informant can be established by showing that the informant has as many of the following characteristics as possible:

- no record of criminal activity
- history of reputable employment
- established resident of the community
- good citizen
- any other indications of honesty and integrity

(9) Special agents should carefully evaluate information provided by informants. The decision to use an informant is sensitive and requires the agency to perform due diligence concerning the background of the individual who will be providing information or receiving direction from the IRS. Internal Revenue Manual 9.4.2, Sources of Information, addresses numerous suitability factors to consider in evaluating informants. The background, motivation, history of providing reliable information, and ability to independently corroborate testimony are all important factors which the special agent, SAC, CT Counsel, and the attorney for the government must consider in evaluating an informant's credibility.

(10) After presenting the facts in a documentary manner, the special agent will summarize the evidence and draw conclusions that ultimately establish probable cause. The conclusion section will specifically state who violated the law, what criminal statutes were violated, where the evidence of the violation exists, and when the violations occurred. Almost every CI search warrant can be described as a financial search warrant because the purpose of any such warrant is to seize financial records. Due to the unique nature of financial investigations, the courts allow the affiant to draw conclusions based upon the special agent's experience and expertise, as well as the available documentary evidence. For example, based upon his/her experience in other investigations, the affiant may draw conclusions about the normal industry practices or the location and types of records that a particular business or individual may keep. Conclusions are not considered probable cause; instead, they support the finding of probable cause.

(11) Throughout the search warrant approval process, the special agent can expect to receive requests for additional information from his/her approving officials. Such requests often seek source documentation to support statements contained within the affidavit. In addition, if the investigation ultimately results in a criminal prosecution, the subject will likely file a motion to suppress the evidence seized pursuant to the search warrant. For these reasons, having a "working copy" of the affidavit, which is organized in such a manner that each line in the affidavit can be traced to supporting documentation can be very helpful. Much like a prosecution recommendation report, but on an informal scale, the working copy of the affidavit is prepared with references. While formal evidence folders are not necessary, some organized means of easily retrieving the source documentation can make the approval and/or motion to suppress processes much simpler. Further, since time is essential to preserving the evidence, the reviews of CT Counsel; the SAC; DOJ, Tax Division; and the attorney for the government will be facilitated by a well-prepared and supported affidavit.

9.4.9.3.1.3
(10-05-2007)
The Description of Items to be Seized

(1) Under the particularity requirement of the Fourth Amendment, the courts consistently hold that the items to be seized must have a nexus to the underlying criminal offenses alleged in the affidavit. Evidence that is seized and found to exceed the scope of the search warrant will be suppressed and declared inadmissible at trial.

(2) When preparing the list of items to be seized, the special agent must be specific as to the nature, type, and time frame of items and records to be seized. Use of "catch-all" phrases, such as " any and all records", will be avoided as they imply an overly broad and non-specific search methodology.

(3) There is an exception to the particularity requirement known as the permeated with fraud theory. If a business is so "permeated with fraud" that there are no records in existence which are devoid of evidence of the underlying criminal offenses, then all the records of the business may be seized. In these instances, the affidavit will specifically state that the business is "permeated with fraud" and describe in sufficient detail why all the records represent evidence of the alleged offenses.

(4) The CIS will provide the proper language to be included describing computer hardware, software, and peripherals to be seized.

a. The search warrant must describe with particularity the hardware components of the computer and the software and data stored within the computer.

9.4.9.3.1.4
(03-17-2011)
The Search Warrant Return

(1) A magistrate judge will review the Application for Search Warrant, along with the affidavit, items to be seized, and a description of the premises to be searched, and will determine if there is probable cause that a crime was committed, that evidence of the crime exists, and that the evidence is located at the particular location specified. If the judge decides that probable cause does exist, he/she will sign the search warrant, authorizing the search of the location specified, for the items specified.

(2) Federal Rules of Criminal Procedure, Rule 41 (e)(2), directs the officer to:

- (i) execute the warrant within a specified time no longer than 14 days;
- (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and
- (iii) return the warrant, including a copy of the inventory, to the magistrate judge designated in the warrant.

(3) The inventories should indicate which items were seized as contraband and also indicate if any items were returned to the custodian. The special agent will obtain a receipt for any items returned to the custodian or turned over to other Federal, state, or local law enforcement officials.

9.4.9.3.2
(03-17-2011)
Planning the Enforcement Action

(1) Any enforcement action, and particularly a CI affiant search warrant, involves extensive preplanning and background work to ensure a safe and efficient operation. For this reason, an SSA may designate a special agent, other than the affiant, to coordinate the enforcement planning aspects of the search warrant.

(2) Support staff will be used to assist in the planning and preparation of enforcement actions; however, due to the unforeseen risks, support staff must not be present at the site where a search warrant is executed.

(3) The participation of a Tax Fraud Investigative Aide (TFIA) is permitted only in IRS affiant search warrants and must be approved by the SAC. The role of the TFIA must be clearly defined in the Plan of Action and Risk Assessment Guide. A TFIA is not allowed, under any circumstances, to enter a search location or physically be waiting in the area of a search location until the premises have been secured. A TFIA must remain at the staging area until the search site has been declared safe by the CI Team Leader. The CI Team Leader on-site has the authority to request the removal of the TFIA if there are any safety concerns or operational issues that arise at any point during the executive of the search warrant.

(4) The following planning documents will be completed for every CI affiant search warrant and can also be found in Document Manager:

- EARF
- Risk Assessment Guide (see 9.4.9.3.2.2 for exceptions)
- Search Warrant Checklist
- Search Warrant Plan

(5) The following planning documents will be completed for search warrants in which CI special agents participate (non-CI affiant):

- EARF
- Risk Assessment Guide (Exhibit 9.4.9-2) will be prepared at the discretion of the SAC. At the least, the SSA should ensure that the executing agency has evaluated the potential risk factors and that CI special agents are assigned appropriate duties.

(6) If items of personal or real property have the potential to be seized for forfeiture purposes, the Asset Forfeiture Coordinator (AFC) will be contacted. See IRM 9.7.4, Pre-Seizure Planning.

9.4.9.3.2.1
(02-09-2005)
Enforcement Action Review Form

(1) In all circumstances where CI is involved in a search warrant that is being executed or served, the EARF is required to establish the basis for the action and to document the SAC's approval of the enforcement action or involvement in the enforcement action.

(2) Only one EARF need be prepared for multiple related sites and/or multiple related enforcement actions on the same investigation/same day.

(3) The narrative to support CI's involvement must be articulated in the appropriate sections of the form, following the criteria established in IRM 9.4.9.2. When one form is prepared for multiple sites, the narrative will contain justification for CI's participation in each site, along with the discussion of intrusiveness for tax investigations. Do not indicate that the reviewer should refer to the affidavit for information. In any enforcement operation, the SAC has the ultimate authority to approve and commit any available sources (except where DFO approval is required for sensitive cases).

9.4.9.3.2.2
(08-02-2010)
Risk Assessment Guide

(1) Completion of the Risk Assessment Guide (RAG) is required for all CI search warrants except those which are served on accounts of a Federally insured bank or financial institution, another Federal agency, or search warrants served via fax or mail. In addition, when CI is the affiant, completion of the RAG is not required for search warrants executed on safe deposit boxes, stock accounts, electronic accounts, and other non-physical locations.

(2) One Risk Assessment Guide will be prepared for each search warrant site.

(3) A Risk Assessment Guide is not required in investigations where CI is assisting other Federal, state, or local agencies; however, at the discretion of the SAC, a Risk Assessment Guide may be warranted.

(4) Special agents may fully participate in every aspect of an enforcement action involving medium or low risk CI search warrants.

(5) If a determination is made that entry into a premises or structure presents a high risk situation, special agents will not engage in the entry. Other means, such as the use of specially trained entry teams from other local, state, or Federal agencies will be considered. In these situations, once entry is made and the location is secured, special agents will then be permitted to enter and complete the search.

9.4.9.3.2.2.1
(02-09-2005)
Criteria of a Low Risk Situation

(1) Low risk situations are those in which it is unlikely that the risk factor/enforcement action could result in a non-permanent physical injury to the special agent or others.

9.4.9.3.2.2.2
(02-09-2005)
Criteria of a Medium Risk Situation

(1) Medium risk situations are those in which it is possible that the risk factor/enforcement action could result in a non-permanent physical injury to the special agent or others. Special agents have the requisite training to deal with these situations and, as such, are authorized to make entry. An example of a medium risk situation is the presence of a firearm, absent other knowledge of intent or criminal history, at a location.

9.4.9.3.2.2.3
(02-09-2005)
Criteria of a High Risk Situation

(1) High risk situations are those in which it is probable that the risk factor/enforcement action could result in death or serious physical injury to the special agent or others. As stated above, CI special agents will not participate in the entry of a location, in high-risk situations. Those circumstances which create a high risk situation include the following:

- presence of booby traps
- presence of a barricaded or fortified location
- need for tear gas
- need for explosive breaching
- toxic/hazardous environment
- presence of sophisticated weaponry
- evidence of premeditated acts of violence against law enforcement officers
- combined with the known ability of occupants to offer armed resistance to entering agents
- prior history of violent criminal behavior, combined with the known ability of occupants to offer armed resistance to entering agents.
- any set of facts which lead the special agent to believe that there is a likelihood of serious physical injury or death unless specialized procedures or equipment are used in the entry

9.4.9.3.2.3
(02-09-2005)
Search Warrant Checklist

(1) The Search Warrant Checklist (see Document Manager) will be prepared for all CI search warrants. Only one Search Warrant Checklist should be prepared for multiple related sites on the same investigation/same day.

(2) A Search Warrant Checklist is not required in investigations where a CI special agent is assisting other Federal, state, or local agencies.

9.4.9.3.2.4
(10-05-2007)
Search Warrant Plan

(1) A Search Warrant Plan, (see Document Manager), will be prepared for all CI search warrants. One search warrant plan will be prepared for each search warrant site.

(2) This plan is not required in investigations where a CI special agent is assisting other Federal, state, or local agencies; however, it is recommended that the operational plan of the other law enforcement entity be made a part of the EARF, along with the special agent's articulation of the need for CI involvement.

9.4.9.3.2.4.1
(02-09-2005)
Executing Searches of Attorney's Offices

(1) The DOJ policy places additional procedures on situations pertaining to the search of the premises of any attorney who is engaged in the practice of law on behalf of clients. The policy is detailed in the United States Attorney's Manual, Title 9, §13.420.

(2) Searches of attorney's offices involve extensive cooperation between CI, CT Counsel, DOJ, and the local US Attorney for the government to ensure compliance with this policy. Additional resources outside the local area may be required that will call for coordination by the SSA.

(3) The policy establishes the use of a "privilege team" consisting of special agents and attorneys who are not directly involved in the underlying investigation. The purpose of the privilege team is to prevent exposing the investigating special agents and prosecuting attorney(s) for the government to privileged material not covered by an exception. Supervisory Special Agent involvement is critical in the early stages to ensure adequate resources. A predetermined set of instructions is given to the privilege team and documented in the search warrant to prevent and limit the exposure to privileged communications, and to ensure that the privilege team does not disclose any information, unless authorized by a privilege attorney, to the investigating special agent(s) and attorney(s) for the government. The privilege team conducts the search and reviews all attorney material that may be privileged. It then determines what materials can be provided to the investigating special agent(s) and prosecuting attorney(s) for the government.

9.4.9.3.2.4.2
(10-05-2007)
Searching and Seizing Computers

(1) The search and seizure of computers is a highly technical and evolving area of search warrant law. The CIS will provide important information with regard to planning the enforcement operation so as to preserve and prevent the destruction of the computerized records and equipment. The lead CIS will coordinate the resources of a CIS team for the search warrant. When the search warrant is executed, the CIS and his/her team will have primary decision making authority and overall responsibility for all computer search and seizure issues (see subsection 9.4.9.6).

9.4.9.3.3
(10-05-2007)
The Approval Process - Criminal Investigation Affiant Search Warrants

(1) A numbered SCI, related to the subject of the search warrant, is required when CI is the affiant for a search warrant (see IRM 9.4.9.2).

(2) The special agent will forward to his/her SSA the following completed documents:

- Search Warrant Affidavit with list of items to be seized
- Enforcement Action Review Form
- Risk Assessment Form(s)
- Search Warrant Checklist
- Search Warrant Plan(s)

(3) Once the SSA reviews the affidavit and signs the EARF, the documents will be forwarded to local CT Counsel for a formal review.

(4) Criminal Tax Counsel prepares a memorandum addressing the legal sufficiency and intrusiveness for Title 26 and tax-related Title 18 search warrants, as well as the legal sufficiency and probable cause in non-tax search warrants. The SSA forwards to the SAC (through the Assistant Special Agent in Charge (ASAC) if appropriate) the following:

- Search Warrant Affidavit
- Enforcement Action Review Form
- Risk Assessment Form(s)
- Search Warrant Checklist
- Search Warrant Plan(s)
- Criminal Tax Counsel's Review Memorandum

Note: Refer to subsection 9.4.9.3.3.3 if the subject is one which requires DOJ, Tax Division approval of Title 26 and tax-related Title 18 search warrants. These search warrants will require an additional level of review.

(5) Final approval authority for CI search warrants rests with the SAC and/or his/her designee. Differences of opinion between CT Counsel and the SAC regarding legal sufficiency and/or intrusiveness will be resolved by the Director, Field Operations.

9.4.9.3.3.1
(02-09-2005)
Criminal Tax Review

(1) Criminal Tax Counsel will review all CI search warrants for legal sufficiency and probable cause. In Title 26 and tax-related Title 18 money laundering investigations, CT Counsel will also evaluate the intrusiveness issue. Subsequent to his/her review, CT Counsel will provide written advice to the SAC for his/her consideration in the search warrant approval process.

9.4.9.3.3.2
(10-05-2007)
Director, Field Operations Concurrence

(1) The SAC is required to obtain written concurrence from the respective Director, Field Operations, for the execution of a search warrant in a sensitive investigation (as defined in IRM 9.4.1 (see Approving a Subject Criminal Investigation)).

(2) The SAC will obtain written concurrence from the respective Director, Field Operations, when a search warrant which targets an individual requiring DOJ, Tax Division approval is being considered (see IRM 9.4.9.3.3.3 below). Criminal Tax Counsel review is required prior to forwarding the search warrant to the Director, Field Operations for concurrence.

9.4.9.3.3.3
(03-17-2011)
Department of Justice, Tax Division Approval

(1) Pursuant to DOJ, Tax Division, Directive No. 52, the local United States Attorneys Office can approve most Title 26 and tax-related Title 18 search warrants. However, DOJ, Tax Division retains exclusive authority to approve Title 26 and tax-related Title 18 search warrants directed at offices, structures, or premises owned, controlled, or under the dominion of a subject of an investigation who is:

- an accountant
- a lawyer
- a physician
- a local, state, Federal, or foreign public official or political candidate
- a member of the clergy
- a representative of the electronic or printed news media
- an official of a labor union
- an official of an organization deemed to be exempt under 26 USC §501(c)(3)

(2) It should be expected that due to the sensitivity of these professions, this additional scrutiny may require a longer period of review. As soon as possible, the SSA should consult with a CT Counsel and DOJ, Tax Division attorney for general guidance on questions regarding the language and details of the affidavit. General questions that can be resolved early will facilitate the review process. However, the specifics of the investigation cannot be disclosed to the DOJ, Tax Division attorney until the SAC makes a referral to the DOJ, unless the case is being investigated by a grand jury.

(3) Once the SAC concurs with the search warrant (signed the EARF) and advises the Director, Field Operations of the proposed action, the following documents will be forwarded to DOJ, Tax Division as a referral:

- Cover letter from the SAC referring the application for a Search Warrant to DOJ, Tax Division for review
- Affidavit for Search Warrant
- Division Counsel/Associate Chief Counsel's (Criminal Tax) Review Memorandum

Note: A simultaneous referral to the local US Attorneys Office can facilitate the process.

9.4.9.3.4
(01-23-2008)
The Approval Process - Non-Criminal Investigation Affiant Search Warrants

(1) Special agents can assist other agencies in the execution of a search warrant, including interviewing subject(s) and related individuals during the execution of the search warrant, with an approved PI. See IRM 9.4.1, General, Primary and Subject Investigations. However, CI cannot interview third party and/or subjects after the execution of another agencies search warrant without a numbered SCI.

(2) The special agent will forward to his/her SSA the following completed documents:

- EARF
- Other Agency's Risk Assessment Form(s) if available
- Other Agency's Search Warrant Plan(s) if available

(3) Once the SSA approves the EARF, it will be forwarded to the SAC (through the ASAC if appropriate). A SAC approved EARF is required prior to a special agent's participation in a non-CI search warrant.

(4) The EARF should address officer safety and training issues that may differ between search warrants of another Federal agency and search warrants of state and local police departments.

(5) In non-CI search warrants (those involving another Federal agency) that are determined to be either a medium or low risk situation, the SAC will ultimately determine the scope and structure of CI's involvement by the totality of the circumstances. If CI is actively involved in the investigation, it is recommended and encouraged that special agents be allowed to fully participate in the enforcement action.

(6) In non-CI search warrants (state and local) that are determined to be either a medium or low risk situation, the SAC, using more scrutiny, will ultimately determine the special agent's involvement based upon the totality of the circumstances. Generally, the special agent will not be a part of the entry team and will be in a security or observer role. In an observer role and due to liability issues, special agents must ensure he/she has read the search warrant and items to be seized so that he/she is in a position to advise as to the value of financial documents. Criminal Investigation special agents will not be assigned to the evidence custodian or seizing officer roles. Based upon an articulation of facts, and if extenuating circumstances exist, the SAC can determine if more in-depth involvement is warranted. The EARF must address and contain sufficient information to substantiate the dedication of resources. Information to consider may include, but is not limited to, the number of sites to be searched in comparison to available resources, the number of personnel committed by each agency, the possibility of remote locations where local or Federal law enforcement officer (LEO) presence is limited, and the need to develop relationships with other LEOs.

9.4.9.3.5
(10-05-2007)
Executing Search Warrant Procedures – Criminal Investigation Affiant Search Warrants

(1) The SAC will be notified prior to changes in the approved date and time of the execution of the search warrant.

(2) All GS-1811 employees and their managers taking an active, participating role should wear a ballistic vest. The final judgment on whether a ballistic vest must be worn, or whether an exception will be granted, rests with the SSA of the enforcement operation or the search warrant team leader when a SSA is not present (see IRM 9.1.4, General, Primary and Subject Investigations).

(3) Special agents should review 18 USC §3109 to make a valid entrance. If the door is broken upon entry, the government may be required to pay to repair the damage.

(4) Upon entry, the premises must be secured and the search warrant will be read to whoever is in control of the premises.

(5) Assigned special agents will photograph and/or video each site location to identify the condition of the premises upon entry and to assist in identifying the location of evidence seized. Next, the premises will be sketched and rooms labeled.

(6) The volume of records normally seized in a financial search warrant requires a detailed inventory. The CI search warrant computer inventory should be utilized.

(7) Document Manager contains the necessary evidence labels, chain of custody forms, and evidence tracking documents. All evidence that is within the scope of the search warrant will be affixed with the IRS, Criminal Investigation evidence tag.

(8) When a computer is at the site during the execution of a search warrant the following must be considered:

- Preserve the chain of custody and integrity of the evidence.
- Pre-programmed destructive software can alter and delete data.
- Determine where the information is being seized: a local personal computer, a network computer, or a computer located outside the United States. Generally, do not seize electronic evidence located outside the United States.
- If applicable, work as directed by the magistrates segregation plan.
- Thoroughly document and photograph the area. Photograph the components of the computers and the cable connections.
- Obtain express authority to remove the computer from the site to conduct the search (if not previously granted.)
- Consult attorneys after encountering issues such as Privacy Protection Act material.

9.4.9.3.5.1
(02-09-2005)
Chain of Custody

(1) Chain of custody is the preservation by successive custodians of the evidence of a crime or any relevant writing in its original condition. Documents or other physical objects may be the instruments used to commit a crime and are generally admissible as such. However, the trial judge must be satisfied that the writing or other physical object is in the same condition as when the crime was committed.

(2) In financial investigations, it may be months or years between the time the evidence is obtained and judicial proceedings. During this time, the documents or other physical objects may have been transferred between two or more special agents or several different special agents may have accessed the original evidence. In order for documents or other physical objects to be admissible as evidence, it is necessary to prove the items are in the same condition as when they were seized, since failure to maintain the evidence in its original condition could jeopardize admissibility.

(3) The custody and storage of seized computers requires additional precautions. The investigating special agent along with the CIS are both responsible to see that the following is maintained in relation to computers:

- Maintain the chain of custody.
- Maintain the integrity of the evidence.
- Follow court ordered segregation plans.
- Document examinations of the computer.
- Return seized items as quickly as possible (if applicable). Obtain a receipt for returned items.

9.4.9.3.5.2
(02-09-2005)
Identification of Evidence

(1) The witness through whom the instrument is to be introduced into evidence must be able to identify it as being in the same condition as when it was recovered.

a. Special agents must, therefore, promptly identify and preserve, in its original condition, all evidentiary material that may be offered into evidence. This would particularly apply to records, recordings, videotapes, documents, and other paraphernalia.
b. Evidence custodians must document and track the transfers of original evidence to establish the chain of custody from initial discovery to the time of judicial proceedings. If original evidence requires examination and analysis by a forensic examiner, the laboratory personnel must maintain their own internal chain of custody procedures. The evidence custodian is only responsible for tracking the original evidence to and from the forensic examiner or laboratory.
c. Access to original evidence should be kept to a minimum in order to preserve the evidence in its original condition.
d. Preferably, original evidence should be handled only twice (i.e., when it is gathered and when it is copied). The special agent may then use the copy of the item of evidence while preserving the original from being lost, stolen, or altered.

(2) In order that a seized item may be admissible as evidence, it is necessary to prove that it is the same item that was seized and is in the same condition as when it was seized. Since several persons may handle the evidence in the interval between the seizure and the judicial proceedings, it should be adequately marked at the time of seizure for later identification.

a. A special agent who seizes documents or other evidence must immediately identify them by completing all the required information on the evidence tag, including the identity of the person(s) who witnessed the discovery of the evidence. The special agent should then affix a completed IRS CI Evidence Tag to an evidence container (envelope, bag, box, carton, plastic bag, etc.) or the evidence itself. This is the normal procedure for items found during a search warrant. This will allow the official evidence custodian to later testify that this is the same evidence that was seized and is in the same condition as it was at the time of seizure.
b. If circumstances indicate the marking of original evidence may render the evidence subject to attack on the grounds it has been defaced or is not in the same condition as when seized, the special agent may make a photostat or other copy of the original evidence for markings, comparisons, or for use as an exhibit to his/her report. The special agent should then return the original evidence to its storage container.

9.4.9.3.5.3
(02-09-2005)
Seizing Contraband, Weapons, Currency, and Other Items

(1) Contraband is any property that is unlawful to possess. Narcotics, stolen property, and other contraband should be photographed, seized, and recorded on a separate inventory. When possible, an appropriate Federal or local law enforcement agency should be called to the search warrant scene to take custody of the contraband.

(2) Weapons are not necessarily contraband. When found at search warrant sites, weapons should be cleared and secured. If there is a question as to whether a firearm is contraband, contact should be made with the local Bureau of Alcohol, Tobacco and Firearms (ATF) office. If weapons are legally owned, they should be returned to the rightful owner at an appropriate time after the execution of the search warrant.

(3) Currency seized for forfeiture or as evidence falls within prescribed the procedures of IRM 9.7.6, Custody and Storage of Seized Assets. Special agents should review the IRM section for the proper procedures for the handling of currency at search warrant sites. The field office AFC must be notified when currency is seized to ensure the proper storage/deposit of the funds.

(4) Evidence not covered within the scope of the search warrant can only be seized by obtaining a new search warrant or from obtaining the consent of the owner of the property. Form 6884, Voluntary Consent to Search of Person, Premises or Conveyances, (see Document Manager), should be included in the search warrant kit for such instances. Proper planning will foresee outbuildings, garages, vehicles, etc. that will require a separate search warrant.

(5) For computer and/or electronic evidence such as computer hard drives, floppy disks, and computer compact discs (CDs), the evidence will be transferred to the CIS agent. Audio and videotapes should be transferred to the technical equipment agent. These technical personnel have the expertise and specialized training in the proper custody and analysis of such evidence. After processing, he/she can either maintain the original evidence or transfer it to the investigating special agent/evidence custodian along with the working copies that have been processed.

(6) Exit photographs and/or video should be taken to document the condition of the premises at the conclusion of the search. A copy of the search warrant and inventory (not the affidavit) will be left at the premises or with a person in control of the premises. The site will be secured before the team leader leaves the premises.

9.4.9.3.6
(03-17-2011)
Post Operation Search Warrant Procedures

(1) Following the execution of the search warrant, the special agent, pursuant to Fed. R. Crim. P. R 41, will return the search warrant, with an inventory of the items seized, to the issuing magistrate. This return must be done promptly.

(2) The special agent (team leader) will also prepare the Post Enforcement Operation Summary Form, (Exhibit 9.4.9-3), for each search warrant site, as soon as possible. This form is mandatory for all CI search warrants, not just tax, or tax-related search warrants.

(3) Criminal Tax Counsel will be provided with a copy of the inventory to conduct a post search warrant inventory review for all search warrants obtained in Title 26 and tax-related Title 18 investigations. Criminal Tax Counsel will not conduct an inventory review for search warrants obtained in pure money laundering investigations.

(4) A copy of the inventory will be given to the local AFC to ensure that required items are identified and properly inventoried on the Asset Forfeiture Tracking and Retrieval System (AFTRAK).

9.4.9.3.6.1
(02-09-2005)
Preserving the Chain of Custody

(1) In order to preserve, in its original condition, all evidentiary material that may be offered into evidence, seized material such as records, recordings, videotapes, document, and other physical objects should be tracked so the custody and control of the evidence can be documented at all times.

(2) Evidence Tag Log forms will be used to record and track the transfer of evidence. Such forms will also be used jointly with Form 13437, National Forensic Laboratory Request for Service, to record the chain of custody

transfer of evidence to a forensic examiner or laboratory. This form was designed for use when any evidence is transferred from one custodian to another. It also enables a custodian to keep track of and retain multiple chain-of-custody forms. For example, use of the form will show a change in an investigating special agent/custodian, transfer of evidence to a forensic examiner or laboratory for analysis, or a temporary transfer of evidence to an AUSA for presentation in a judicial proceeding.

(3) The Evidence Access Control Log form is designed to record and document **all** access to controlled areas where evidence is stored. The form is formatted to record access to the storage location or a specific evidence storage container such as a wire cage, file cabinet, envelope, box, etc. The official evidence custodian is required to record an access entry no more than one time per day. Everyone else is required to record an access entry for each and every instance when they enter the controlled access area. The "notes" section for each access entry, except those for the official evidence custodian, is used to record specific information about the purpose for entering the controlled access area, identify what evidence was accessed, and specify the reason for accessing the evidence. The form is kept with the evidence at the secured storage location.

9.4.9.3.6.2
(02-09-2005)
Transfer of Evidence

(1) The investigating special agent may request laboratory examination of certain items of evidence. In selecting evidence to be sent to an examiner or laboratory for examination, it may be necessary to remove a selected item from its storage container.

a. A clearly marked, clean, first generation photocopy of all evidence submitted to the laboratory should be retained in the storage container as a substitute record of items removed and as a record of the condition of these items when they were sent for laboratory analysis. In some instances, ink chemistry and/or latent print examinations will adversely affect the original appearance of the evidence.
b. The transfer of items for forensic examination or analysis should be recorded on the Evidence Tag form. The form must accompany the evidence along with Form 13437. A copy of both forms should be placed in the evidence storage container(s) along with the copy(s) of removed documents/evidence.
c. Descriptions of evidence submitted to the examiner or laboratory should be sufficient so that items which are similar in appearance can be distinguished.
d. "Questioned" and "known/acknowledged " items of evidence should be packaged in separate sealed containers. There are instances where it may not be clear to the examiner or laboratory employees whether normal course of business records are being submitted as "known" or "questioned" items of evidence. "Known" items of evidence can be returned to the investigating special agent after examination while "questioned" items of evidence require further analysis.
e. Package rolled ink or electronically scanned fingerprint cards in a separate envelope.
f. Write on the evidence tag and/or storage container **prior** to putting any evidence in the container. This will prevent accidental impressions on the evidence.
g. **Do not** place laboratory request forms, descriptions of evidence, and any chain of custody forms inside of sealed containers holding "questioned" or

" known/acknowledged" evidence. Attach the forms to the outside of evidence container so the evidence container seal is in tact until it is time for processing the evidence.

9.4.9.4
(03-17-2011)
Uniform Policy for Search Warrant File Maintenance

(1) In all instances where a CI special agent is an affiant, the following documents will be maintained electronically by the originating group:

a. Signed Affidavit for Search Warrant
b. Signed Search Warrants with all attachments
c. Ex Parte Orders (Order for tax disclosure in non-tax cases)
d. CT Counsel's pre and post review documents
e. Enforcement Action Review Form
f. Risk Assessment Guide for each search warrant site
g. Search Warrant Checklist
h. Search Warrant Pre-Operational Plan
i. Post Enforcement Operation Summary
j. Signed Search Warrant return, including an inventory of the items seized from each search warrant location

(2) The above documents must be maintained in the originating group's administrative investigation file. While such documents will ideally be kept in an electronic format, it is understood that paper documents may be more practical in some instances. Regardless of the format, these documents should be readily accessible for investigative purposes and properly "retired" (i.e., stored) with related investigation files when the investigation is closed.

(3) In addition to the documents maintained in the group files, a copy of the Enforcement Action Review Form must be maintained in the SAC's administrative files. These "centralized" files may also be electronic, paper, or a combination thereof. However, they must be readily accessible indefinitely for internal or external review.

(4) In all instances where a CI special agent is a participant in another agencies search warrant, the EARF is the only document that is required to be maintained in the SAC's electronic administrative files.

9.4.9.5
(10-05-2007)
Search Warrants and Less Intrusive Methods for Obtaining 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.

9.4.9.5.1
(10-05-2007)
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 DOJ); and a court order obtained in accordance with 18 USC §2516 and 18 USC §2518. See IRM 9.4.6, Surveillance and Non-Consensual Monitoring.

9.4.9.5.2
(10-05-2007)
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.

9.4.9.5.3
(10-05-2007)
Judicial Process for Obtaining Stored Electronic Communications, Transactional Information, and Subscriber Information

(1) Title 18 USC §2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information such as account records and basic subscriber information.

(2) Title 18 USC §2703 offers five mechanisms that a " government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms, in ascending order of required threshold showing, are as follows:

a. subpoena
b. subpoena with prior notice to the subscriber or customer
c. 18 USC §2703(d) court order
d. 18 USC §2703(d) court order with prior notice to the subscriber or customer
e. search warrant

(3) One feature of the compelled disclosure provisions of Electronic Communications Privacy Act (ECPA) is that greater process generally includes access to information that can be obtained with lesser process. Thus, a 18 USC §2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 18 USC §2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified, both because it can authorize a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the statute. Note, however, the notice requirement must be consid-

ered as a separate burden under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a 18 USC §2703(d) order without subscriber notice. (One small category of information can be compelled under the ECPA without a subpoena. When investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing. See 18 USC §2703(c)(1)(D)).

9.4.9.5.3.1
(10-05-2007)
Subpoena

(1) Investigators can subpoena basic subscriber information. The ECPA permits the government to compel two kinds of information using a subpoena. First, the government may compel the disclosure of the basic subscriber information (discussed above) listed in 18 USC §2703(c)(2):

a. name
b. address
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
f. means and source of payment for such service (including any credit card or bank account number)

9.4.9.5.3.2
(10-05-2007)
Subpoena With Prior Notice to the Subscriber or Customer

(1) Investigators can subpoena opened e-mail from a provider if they comply with the notice provisions of 18 USC §2703(b)(1)(B) and 18 USC §2705. This notice is not the notice required under 26 USC §7609(a)(3)(A), third-party recordkeepers. In general, internet service providers are not third-party recordkeepers.

(2) Agents who obtain a subpoena, and either give prior notice to the subscriber or comply with the delayed notice provisions of 18 USC §2705(a), may obtain:

a. everything that can be obtained using a subpoena without notice
b. "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." - 18 USC §2703(b)(1)(B)(i), 18 USC §2703(b)(2); and
c. "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." - 18 USC §2703(a)

(3) As a practical matter, this means that agents can obtain opened e-mail (and other stored electronic or wire communications in "electronic storage" the more than 180 days) using a subpoena, so long as they comply with the ECPA's notice provisions. See House of Representatives, Public Law 99-647, at 64-65 (1986).

(4) The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. See 18 USC §2703(b)(1)(B). However, 18 USC §2705(a)(1)(B) and 18 USC §2705(a)(4) permit notice to be delayed for 90 days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." - 18 USC §2705(a)(1)(B)

9.4.9.5.3.3
(10-05-2007)
Title 18 USC 2703(d) Order

(1) Special agents need a 18 USC §2703(d) court order to obtain most account logs and most transactional records.

(2) Special agents who obtain a court order under 18 USC §2703(d) may obtain:

a. Anything that can be obtained using a subpoena without notice.
b. All "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." - 18 USC §2703(c)(1)
c. A court order authorized by 18 USC §2703(d) may be issued by any Federal magistrate, district court or equivalent state court judge. See 18 USC §2703(d), 2711(3). To obtain such an order, known as an " articulable facts" court order or simply a "d" order.

(3) The governmental entity must offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

(4) This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order.

9.4.9.5.3.4
(10-05-2007)
Title 18 USC §2703(d) Order with Prior Notice to the Subscriber or Customer

(1) Investigators can obtain everything in an account except for unopened e-mail or voice mail stored with a provider for 180 days or less using a 18 USC §2703(d) court order that complies with the notice provisions of 18 USC §2705.

(2) Agents who obtain a court order under 18 USC §2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of 18 USC §2705(a), may obtain:

a. Everything that can be obtained using a 18 USC §2703(d) court order without notice.
b. "The contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," - 18 USC §2703(b)(1)(B)(ii), 18 USC §2703(b)(2)
c. "The contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." - 18 USC §2703(a). As a practical matter, this means that the government can obtain the full contents of a subscriber's account except unopened e-mail and voice mail (which has been in "electronic storage" 180 days or less) using a 18 USC §2703(d) order that complies with the prior notice provisions of 18 USC §2703(b)(1)(B).

(3) As an alternative to giving prior notice, agents can obtain an order delaying notice for up to 90 days when notice would seriously jeopardize the investigation. In such cases, agents generally will obtain this order by including an appropriate request in the agents' 18 USC §2703(d) application and proposed order. The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger the life or physical safety of an

individual; lead to flight from prosecution; lead to destruction of or tampering with evidence; lead to intimidation of potential witnesses; or . . . otherwise seriously jeopardize an investigation or unduly delay a trial." Importantly, the applicant must satisfy this standard anew every time the applicant seeks an extension of the delayed notice.

9.4.9.5.3.5
(10-05-2007)
Search Warrant

(1) Investigators can obtain the full contents of an account with a search warrant. The ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

(2) Special agents who obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure (Fed. R. Crim. P. R41) or an equivalent state warrant may obtain:

a. everything that can be obtained using a 18 USC §2703(d) court order with notice
b. "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." - 18 USC §2703(a)

(3) In other words, agents can obtain every record and all of the contents of an account by obtaining a search warrant based on probable cause pursuant to Fed. R. Crim. P. R41. The search warrant can then be served on the service provider and compels the provider to divulge to law enforcement the information described in the search warrant. Notably, obtaining a search warrant obviates the need to give notice to the subscriber. See 18 USC §2703(b)(1)(A).

(4) 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. Exhibit 9.4.9-1 is a sample of a 18 USC §2703(f) "Preservation Letter".

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.
b. The authority to direct providers to preserve records and other evidence is not prospective. That is, 18 USC §2703(f) letters can order a provider to preserve records that have already been created, but cannot order providers to preserve records not yet made. If agents want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes discussed in IRM 9.4.6, Surveillance and Non-Consensual Monitoring.

9.4.9.5.4
(08-02-2010)
Approval/Authorization for Stored Electronic Communications, Transactional Information, and Subscriber Information

(1) The investigating special agent should consult with the local 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, Request for Stored Electronic Communication/Transactional Information/Subscriber Information. After SAC approval, the Form 9809 must be forwarded electronically to Special Investigative Techniques (CI:OPS:SIT) and Electronic Crimes (CI:TOIS:EC) 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.

9.4.9.5.5
(10-05-2007)
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 and a copy to CI:TOIS:EC. 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.

9.4.9.6
(10-05-2007)
Computer Searches and Seizures

(1) The search and seizure of data contained in computers, computer networks, and other electronic storage mediums (such as "e-mail") present special circumstances for consideration to insure the legality of the search and seizure. Special agents should possess a working knowledge of the fundamental rules of evidence, that are applicable to the execution of computer search warrants. This subsection covers the following topics:

- Computer Evidence
- Probable Cause and Preparation of Search Warrant
- The Approach and Search
- Custody and Storage of Seized Property

9.4.9.6.1
(10-05-2007)
Computer Evidence

(1) Special agents must use the least intrusive means possible to obtain evidence. Electronic information can be obtained by consent, subpoena, or search warrant.

(2) Consent searches must be voluntarily given and may be limited in scope. Seek consent from the target, employer, or other party with authority established by law. Also see Searches Made With Consent located in IRM 9.4.9, Search Warrants, Evidence, and Chain of Custody.

(3) Always consider the use of a subpoena for computer information not under the control of the target. Subpoena computer records as they exist at the time of service of the subpoena. Direct the recipient to make and safeguard a copy of the requested information, even if they intend to contest the subpoena. Subpoena targets for passwords and encryption keys. A grant of act production immunity may be required.

(4) When deciding whether to search and/or seize one or more computers, there are several issues to consider. Confront the issues early in the investigation if possible. Coordinate procedures relating to pre-search, search, and post search activities with the special agent/computer investigative specialist.

9.4.9.6.2
(10-05-2007)
Applicable Law

(1) Several laws and regulations govern obtaining evidence from electronic sources. These statutes impose restrictions and obligations on the special agent and any operator of public computer services. Review the following before attempting to obtain evidence from electronic sources:

a. First Amendment to the Constitution
b. Fourth Amendment to the Constitution
c. Wiretap Act, 18 USC §2510-2521
d. Electronic Communications Privacy Act of 1986, 18 USC §2701–2711
e. Privacy Protection Act, 42 USC §2000aa
f. Fed. R. Crim. P. R41
g. Federal Rules of Evidence, Sections 901, 1001, and 1002
h. IRM 9.4.9, Search Warrants, Evidence, and Chain of Custody

9.4.9.6.3
(10-05-2007)
Additional Information

(1) Obtain additional information to secure evidence from computers and other electronic media from the following sources:

a. Internet Investigation Guidelines written by CI
b. Computer Investigative Specialist
c. Federal Guidelines for Searching and Seizing Computers published by the DOJ
d. Internet Investigation Guidelines published by the DOJ
e. Division Counsel/Associate Chief Counsel (Criminal Tax)
f. Computer and Telecommunications Coordinators at the local US Attorney's Office or Assistant US Attorneys that have received special training in the computer crimes subject area
g. Tax Division, DOJ: Senior Trial Attorney
h. Computer Crime and Intellectual Property Section, DOJ

9.4.9.7
(10-05-2007)
Probable Cause and Preparation of Search Warrant

(1) When it is anticipated that a computer is on site, the following issues should be considered when obtaining a search warrant. It is recommended that the special agent and special agent/computer investigative specialist discuss the following pre-search considerations:

a. The best evidence is a paper document or paper computer print out.
b. Obtain information about the subject'(s) use of computers before the search.
c. Determine the role of the computer in the offense.
d. Develop probable cause for evidence contained in computers.
e. Develop probable cause for each component of the computer.
f. Participate with the special agent/computer investigative specialist in technical interviews that include computer issues.
g. Consult Counsel and/or the US Attorney's office on computer issues during the investigation.
h. The warrant must describe with particularity the places to be searched and the items to be seized. Describe the hardware components of the computer and the software and data domiciled within the computer.
i. Focus the search warrant affidavit on the evidence sought from the computer. The agent must articulate a factual basis to believe that the computer was used for the creation and/or storage of evidentiary records.
j. Explain in the affidavit why an on-site search is not reasonable and seek permission to seize the computer and search it later, if applicable.
k. Investigate the possibility of protected material on the computer. Include a positive statement in the warrant that no "work product material" exists on the computer.
l. If protected material exists on the computer, state how the protection is not going to be violated. Magistrates can authorize a segregation plan.
m. Investigate the possibility of e-mail on the computer. Indicate the e-mail

status in the search warrant affidavit and the search warrant. Identify in the warrant whose e-mail is going to be read, and if it is subject to search (see 18 USC §2703).

n. Obtain a "no-knock warrant" if destruction of stored computer data is a concern.

9.4.9.8
(10-05-2007)
The Approach and Search

(1) Consider the following search issues during the execution of the warrant when a computer is on site:

a. Preserve the chain of custody and integrity of the evidence.
b. Pre-programmed destructive software can alter and delete data.
c. Determine where the information is being seized from: a local personal computer, a network computer, or a computer located outside the United States.
d. Generally, do not seize electronic evidence located outside the United States.
e. If applicable, work as directed by the Magistrate's segregation plan.
f. Thoroughly document and photograph the area. Photograph the components of the computers and the cable connections.
g. Obtain express authority to remove the computer from the site to conduct the search (if not previously granted.)
h. Consult attorneys after encountering issues such as Privacy Protection Act material.

9.4.9.9
(10-05-2007)
Custody and Storage of Seized Property

(1) Consider the following search issues after the execution of the warrant in relation to computers:

a. maintain the chain of custody
b. maintain the integrity of the evidence
c. follow court ordered segregation plans
d. document examinations of the computer
e. return seized items as quickly as possible (if applicable)
f. obtain a receipt for returned items

Exhibit 9.4.9-1 (10-05-2007)
Sample 18 USC §2703(f) "Preservation Letter"

United States District Court

(ENTER JUDICIAL DISTRICT)

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT

CASE NUMBER:

I being duly sworn depose and say:
I am a(n) Special Agent, Criminal Investigation
Internal Revenue Service, U.S. Treasury
Official Title
and have reason to believe
that ☐ on the person of or ☐ on the property or premises known as (name, description and/or location)

in the Judicial District of (ENTER JUDICIAL DISTRICT)
there is now concealed certain property, namely

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

concerning a violation of Title United States code, Section(s)
The facts to support a finding of Probable Cause are as follows:

Continued on the attached sheet and made a part hereof. ☐ Yes ☐ No

Signature of Affiant

Sworn to before me, and subscribed in my presence

Date at City and State

United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

Page 1 of 2

Exhibit 9.4.9-1 (Cont. 1) (10-05-2007)
Sample 18 USC §2703(f) "Preservation Letter"

UNITED STATES DISTRICT COURT

(ENTER JUDICIAL DISTRICT)

(ENTER DIVISION)

IN THE MATTER OF SEARCH WARRANT FOR THE PREMISES OF	§	
	§	MAGISTRATE NO.
	§	
LOCATED AT	§	
	§	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

LOCATIONS TO BE SEARCHED

AFFIANT EXPERIENCE

AFFIANT'S KNOWLEDGE

BACKGROUND

ITEMS TO BE SEIZED

CONCLUSIONS OF AFFIANT

_____

Special Agent, IRS-CI

Subscribed and sworn to before me

this _____ day of _____, _____.

_____

UNITED STATES MAGISTRATE JUDGE

Exhibit 9.4.9-2 (08-02-2010)
Risk Assessment Guide

Voluntary Consent to a Search of Person, Premises, or Conveyance

Statement of Rights

Before we search your premises (or person or conveyance) you should be aware of your rights under the Fourth Amendment to the Constitution.

You have the right to refuse to permit us to enter your premises (or to search your person or conveyance).

If you voluntarily permit us to enter and search your premises (or to search your person or conveyance) any incriminating evidence that we find may be used against you in court, or other proceedings.

Prior to permitting us to search, you have the right to require us to secure a search warrant.

Waiver

I have read the above statement of my rights and, fully understanding these rights, I waive them freely and voluntarily, without threat or intimidation and without any promise of reward or immunity.

Person, premises or conveyance to be searched:

Location of search:

Date:

Time:

Witness:

Name

Name

Name

Special Agent

Title

Form **6884** (8-82) Department of the Treasury - Internal Revenue Service

Exhibit 9.4.9-2 (Cont. 1) (08-02-2010)
Risk Assessment Guide

Enforcement Action Review Form

1) GENERAL INFORMATION

A. Field Office	**B.** Date
C. Subject Name ***(Last, First, M)***	**D.** Occupation
E. CI Investigation Number ***(if applicable)***	**F.** Special Agent Name

G. Type of Enforcement Operation:
☐ Search Warrant ☐ Arrest Warrant ☐ Seizure Warrant
☐ Other

H. Have the Asset Forfeiture Coordinator, Computer Investigative Specialist and Public Information Officer been notified of pending action?
☐ Yes ☐ No ☐ Not Applicable

I. Proposed Date and Time of Execution

J. Previous Enforcement Action
Date Type

K. Type of Investigation:
☐ Legal Income ☐ Illegal/Non Narcotic ☐ OCDETF
☐ Counterterrorism ☐ Other Explain _____

L. Is a CI special agent the Affiant? ☐ Yes ☐ No
If "no", what is the Affiant's agency?

M. Is CI participation incident to an ongoing task force?
☐ Yes ☐ No
☐ OCDETF ☐ HIDTA ☐ Counterterrorism
☐ Other

N. Address where enforcement action is to be conducted:
Street:
City and State:

Type of location : ☐ Residence ☐ Business ☐ Both
☐ Non-Physical or Secured Location ***(Bank Accounts, Safe Deposit Boxes, etc)*** ☐ Other – Describe
(If there are multiple sites, attach list to synopsis section)

O. Is this a Grand Jury Investigation? ☐ Yes ☐ No

P. Is a Service Initiated Grand Jury Request pending?
☐ Yes ☐ No
(If YES, the proposed grand jury request should be held in abeyance).

2) SPECIAL PERSONS

A. Is this a Title 26 or Title 18 tax-related warrant that pertains to any of the following persons or representatives?

Accountant, Lawyer, Physician, Public Official or Candidate, Clergy, News Media Representative, Labor Union Representative, Exempt Organization Member.

☐ Yes ***(Explain)*** ☐ No
(If yes, CT Counsel review, Director, Field Operations concurrence, and DOJ Tax Division approval is required)

B. Does the warrant pertain to a foreign national?
☐ Yes ☐ No
Agent designated to notify arrestee of their right to Consular access _____
Agent designated to notify the arrestee's embassy _____

C. Do you expect the enforcement action to draw publicity?
☐ Yes ☐ No
☐ National ☐ Regional ☐ Local

D. What is the subject's notoriety in the community?
☐ High ☐ Medium ☐ Low

3) INFORMANT INFORMATION
CRIMINAL INVESTIGATION WARRANT ONLY

	YES	NO
A. Is the primary source of information a confidential informant?	☐	☐
B. Has the confidential informant been paid for information?	☐	☐
C. Has the confidential informant furnished reliable information to CI in the past?	☐	☐
D. Has the information provided by the confidential informant for this warrant been corroborated?	☐	☐
E. If "D" is "no", has a polygraph exam been considered? ***(If "yes", discuss details in explanation section)***	☐	☐
F. Is there documentary evidence to support the confidential informant's information in this instance?	☐	☐
G. Does the confidential informant have a criminal record? ***(If "yes", attach detail in explanation section)***	☐	☐
H. Does another informant corroborate this information?	☐	☐

I. If this informant is not controlled by Criminal Investigation, note the Agency name :

4) COMPLETE FOR NON-TAX CI SEARCH WARRANTS ONLY

A. Are there other methods of acquiring the same evidence? If "yes", explain	☐	☐
B. Is the potential for destruction of evidence likely in this investigation, if this action does not occur?	☐	☐
C. Is contraband expected to be encountered? ***(If "yes" detail in explanation section)***	☐	☐

5) CI TAX AND TAX RELATED WARRANTS ONLY
(Detail on Page 2)

A. Significance Evaluation: Discuss the significance of the case – tax due, nature of the fraud, need for evidence to be seized, anticipated effect on voluntary compliance

B. Intrusiveness Evaluation: Discuss why other investigative methods cannot produce the evidence being sought, and why the search warrant represents the best and least intrusive method to secure the evidence

6) RISK ASSESSEMENT IN CI ENFORCEMENT OPERATIONS

☐ High ☐ Medium ☐ Low
☐ N/A ***(Risk Assessment Guide Not Required)***
(If there are multiple sites, state level for each in synopsis section)
Attach Risk Assessment Guide(s)

7) RISK ASSESSMENT – NON CI WARRANTS

A. How do you rate the physical risk factors of this warrant?
☐ High ☐ Medium ☐ Low
(Explain in detail if High)

B Explain what equipment and attire will be used:

Form 13739 (07-2010)	Cat.#47325A	Page 1 of 3	Department of Treasury-Internal Revenue Service

Exhibit 9.4.9-3 (10-05-2007)
Post Enforcement Operations Summary Form

Enforcement Action Review Form

Synopsis of the Case

(Give a brief description of the case, any unusual circumstances, and the role of CI in the enforcement action.) ☐ Attachment

Additional Explanation Section (Include all information by item number from the first page)

Explanation of Items

Item #	
Item #	
Item #	
Item #	

CI Tax and Tax Related Warrants ☐ Attachment

A) Significance Evaluation

B) Intrusiveness Evaluation

Review/Approval Section

Level	Signature	Date
Reviewed by: Supervisory Special Agent		
Reviewed/Approved by: Assistant Special Agent in Charge		
Approved by: Special Agent in Charge		
Concurrence*: Director, Field Operations	☑	

*The Director, Field Operations must concur in writing with all enforcement actions involving "sensitive investigations." A "sensitive investigation" is defined as an investigation that involves one of the following: a currently serving elected federal official; a currently serving Article III judge; a currently serving high-level Executive Branch official; a currently serving elected statewide official; a currently serving member of the highest court of the state; a mayor currently serving a population of 250,000 or more; perjury in the U.S. Tax Court; an exempt organization.

Enforcement Action Review Form (Rev 12/2002)		Department of Treasury-Internal Revenue Service

Exhibit 9.4.9-3 (Cont. 1) (10-05-2007)
Post Enforcement Operations Summary Form

INTERNAL REVENUE SERVICE - CRIMINAL INVESTIGATION
RISK ASSESSMENT GUIDE

This is a guide for assessing the potential risk in any enforcement operation. It should be prepared by the assigned special agent, reviewed by the Supervisory Special Agent, and approved by the Assistant Special Agent in Charge and/or Special Agent in Charge. Each of the considerations should be commented on in the column provided, with the level of risk (low, medium, or high) entered in the last column. General criteria for evaluating high, medium, and low risk are identified below:

High Risk

High risk situations are those in which it is probable that the risk factor/enforcement action could result in death or serious physical injury to the agent or others. CI agents are not trained to handle high risk enforcement actions. Among circumstances that would create a high risk situation are the following:

- Presence of booby traps
- Presence of a barricaded or fortified location
- Need for tear gas
- Need for explosive breaching
- Toxic/Hazardous environment
- Presence of sophisticated weaponry
- Evidence of premeditated acts of violence against law enforcement officers, combined with the known ability of occupants to offer armed resistance to entering agents
- Prior history of violent criminal behavior, combined with the known ability of occupants to offer armed resistance to entering Agents
- Any set of facts which lead the special agent to believe that there is a likelihood of serious physical injury or death unless specialized procedures or equipment are used in the entry.

If a determination is made that entry into a premises or structure presents a high risk situation, special agents will not engage in the entry. Other means, such as use of specially trained entry teams from other local, state or federal agencies, will be considered. Once entry is made and a location is secured, special agents will be able to enter to complete the search.

Medium Risk

Medium risk situations are those in which it is possible that the risk factor/enforcement action could result in a non-permanent physical injury to the agent or others. Agents have the requisite training to deal with these situations and, as such, are authorized to make entry. An example of a medium risk situation is the presence of a firearm, absent other knowledge of intent or criminal history, at a location.

Low Risk

Low risk situations are those in which it is unlikely that the risk factor/enforcement action could result in a non-permanent physical injury to the agent or others.

Investigation Name:

Investigation Number:

Date and Time of Enforcement Action:

Location/Address of Enforcement Action:

Type of Enforcement Action: ☐ **Search Warrant** ☐ **Arrest Warrant** ☐ **Seizure Warrant** ☐ **Other**

Overall Assessment of Risk for this Enforcement Operation ☐ **Low** ☐ **Medium** ☐ **High**