# Non – Consensual Interception
# Table of Contents

Page

# NON-CONSENSUAL INTERCEPTIONS

## Introduction

This chapter is intended to serve as an operational guide for all agent and technical personnel who engage in the conduct of non-consensual wire or oral communication interceptions. Although most of the non-consensual interceptions which are conducted by this Service are conducted pursuant to the provisions of Titles I and/or III of the Electronic Communications Privacy Act of 1986, as amended (18 U.S.C. 2510, **et seq.**), this Service may, on occasion, conduct non-consensual interceptions pursuant to the provisions of other statutes or executive orders which have a bearing on our protective responsibilities such as the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, et seq.) or Executive Order 12333.

Each of these other statutes or executive orders contains specific provisions for the conduct of communication interceptions. Because the intercept guidelines contained within these other statutes and executive orders are so diverse and so infrequently used by this Service, they are not addressed in this manual. All requests for authorization of communications intercepts which are subject to provisions of statutes or executive orders, other than Titles I and/or III, should be directed to the Intelligence Division. The Intelligence Division will contact the Investigative Support Division (ISD) in these cases to coordinate the conduct of these interceptions and to ensure statistical and record keeping functions.

Prior to preparing for any non-consensual interception, this chapter should be read in its entirety by all agents and supervisory agents who are to be responsible for preparation of the required documentation or who will directly oversee the actual interception operation. Because of the extremely sensitive nature of this type of interception, each employee is cautioned that **any deviation from the policy and procedure set forth in this chapter may subject the employee to disciplinary action, to include dismissal, and may also expose the employee to criminal and/or civil liability.**

## Types of Non-Consensual Interceptions

With the continual advancement of technology, non-consensual interceptions are no longer limited to standard hardwire telephones. They also apply to interceptions of cellular telephone communications, electronics communications (to include e-mail, faxes, internet and digital display pagers) , and interception of dialed numbers using trap/trace devices and pen registers . These interceptions remain governed by all the laws, policies, and procedures set forth in this chapter.

# Preparing for a Non-Consensual Interception

Liaison with the Technical Security Division (TSD) and the Investigative Support Division (ISD) will be established as soon as the decision has been made to apply for a non-consensual interception. TSD will make all necessary coordination with the telephone service providers for the interception of both hard lines and cellular telephone systems. TSD will also determine what equipment will be required and acquire all equipment necessary to conduct the interception. The most up to date telecommunication interception equipment available and capable of intercepting oral communication and call data will be installed on all anticipated target telephone lines. Early installation of the interception equipment will also facilitate the initiation of the interception once it is authorized by the court. ISD will coordinate with the Electronic Surveillance Unit of the Department of Justice (DOJ) and assist the case agent with required ELSUR checks and preparation of Directorate authorization letter. ISD will also maintain a record of electronic interception.

In addition, liaison must be established with the Assistant United States Attorney (AUSA) who will supervise the interception. It is the responsibility of this Assistant United States Attorney to provide guidance in the composition and submission of the required affidavit, application, and court order; and to later provide supervision in the overall conduct of the interception.

# Headquarters Notification of Submission of Application to Department of Justice (Notification Message)

Once a decision is made to apply for a nonconsensual interception (to include interception over digital display pagers), telephone notification should be made to the Technical Security Division (TSD), appropriate operational division, and the Investigative Support Division (ISD). Upon submission of the application to the Department of Justice, an official message will be submitted to Headquarters under the case number of the investigation for which the interception is to be conducted.

The distribution of this official message will include the appropriate operational division, appropriate Assistant Directors office, Technical Security Division (TSD), and Investigative Support Division (ISD). The official message will reference the previous telephone communications between the case agent and Headquarters officials, notifying of the intent to submit an affidavit in support of a non-consensual interception. The following page has a sample official message for reporting the notification.

# Sample Headquarters Notification Official Message Reporting Submission of an Application to the Department of Justice

FROM: SAIC-FIELD OFFICE CASE NUMBER:

CASE TITLE:

TO: SAIC-APPROPRIATE OPERATIONAL DIVISION

INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE
SAIC-INVESTIGATIVE SUPPORT DIVISION
SAIC-TECHNICAL SECURITY DIVISION

SUBJECT: NOTIFICATION OF APPLICATION FOR A NON-CONSENSUAL INTERCEPTION

REFERENCE IS MADE THE TELEPHONE CONVERSATIONS BETWEEN SA_____ (APPROPRIATE FIELD OFFICE), AND SA_____ (APPROPRIATE OPERATIONAL DIVISION), AND SA_____ (ISD), AND SA (PSS) _____ (TSD), REGARDING THE INTENTION TO APPLY FOR A COURT ORDER TO CONDUCT A NON-CONSENSUAL INTERCEPTION.

THIS OFFICIAL MESSAGE IS TO SERVE AS NOTIFICATION THAT AN APPLICATION FOR A NON-CONSENSUAL INTERCEPTION HAS BEEN FORMALLY SUBMITTED TO THE DEPARTMENT OF JUSTICE, AS OF _____ (DATE OF SUBMISSION).

TECHNICAL SECURITY DIVISION IS REQUESTED TO PROVIDE EQUIPMENT AND NECESSARY TECHNICAL ASSISTANCE IN THE TITLE INVESTIGATION.

FIELD OFFICE CASE SA/SUPERVISOR/SAIC

## Types of Cases in Which Authorization May Be Granted

Judicial authorization for a non-consensual interception may be granted if probable cause has been shown in the application and accompanying affidavit(s) that any of the offenses enumerated in 18 U.S.C. 2516 have been, are being, or will be committed.

It should be noted that the applicant's Federal agency must have responsibility for the investigation of the offense for which the application is made as outlined in Title 18, U.S.C., 2516 (1). Offenses not specifically assigned in legislation to another agency may be applied for by the U. S. Secret Service under the provisions of Title 18 U.S.C., Section 3056 (c) (1) (C). For example, this means that the U.S. Secret Service would not be allowed to apply for an interception for a violation of Section 831 pertaining to the prohibited transactions involving nuclear materials since we are not responsible for the investigation of those crimes.

## Overview of the Title I Application Process

The Title I application process begins with an affidavit prepared by the case agent. The affidavit will be reviewed by the AUSA and, based on the affidavit, the AUSA prepares an application for the court order (herein after "application") and a draft court order. The affidavit, application, and draft court order is forwarded to OEO/DOJ for review and approval by the AUSA handling the case. Once the affidavit, application, and draft court order is approved by OEO, ISD will submit a letter in support of the Title I, signed by the Assistant Director. OEO will then submit the documents to the attorney general or his/her designee with the recommendation for approval. Once the attorney general or his/her designee authorizes the Title I interception, OEO will forward the signed authorization to the AUSA in charge of the case. The case agent then will have the court order signed by a judge in the district where the Title I interception will take place.

"Spin off" applications on other subjects or facilities or telephone numbers are handled as separate requests and the process is the same as the initial request.

## Roving Interceptions

18 U.S.C. 2518 (11), (12) established the roving provisions under Title I of Electronic Crimes Privacy Act. These provisions permit the interception of oral, wire, or electronic communications of named subjects without requiring that a specific facility or premises be identified in advance of the authorization.

In the case of a roving oral interception, the application must establish, and the order must specifically find, that probable cause exists that a particular subject is committing a Title I offense at a location that is not practical to specify.

In the case of a roving wire or electronic interception, 18 U.S.C. 2518 (11) (b) (ii) requires probable cause showing that the actions of a named subject could have the effect of thwarting the reception from a specified facility. While the statute does not address the jurisdictional restrictions of roving interceptions, DOJ ruled that a roving interception is not trans-jurisdictional. An order must be obtained in each jurisdiction in which roving interceptions are to be conducted. The exception to this is in the case of mobile cellular telephones or vehicles that cross jurisdictional lines. Title 18, U.S.C. 2518 (3) permits extra-jurisdictional orders and interception. Consultation with an AUSA is advised when a roving interception is considered.

# Applying for a Non-Consensual Interception

There are several steps that must be followed in applying for an interception. Except for emergency authorizations, all of the following documentation must be completed and submitted to the Department of Justice, Office of Enforcement Operations, Electronic Surveillance Unit, through ISD, for review and approval prior to being presented to the presiding judge for approval and issuance of the court order:

1) Affidavit,

2) Application,

3) Court Order,

4) Authorization Request Letter from the Director or his/her designee.

Except for item 4, the Assistant United States Attorney who will supervise the interception should assist the case agent in the composition and submission of these documents.

For the sake of brevity, no sample affidavits, applications, or court orders are included in this manual. Copies of these may be obtained from ISD.

Application for interception of electronic communication and Pen Register and Trap and Trace orders capable of collecting Uniform Resources Locators (URLs) should be forwarded by the AUSA handling the case to the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division, Department of Justice.

## Exception

Prior DOJ approval is required for most applications to conduct interception of electronic communications. An exception was made for electronic communications intercepted over digital display pagers; applications involving digital display pagers may be authorized by an Assistant United States Attorney.

## 1) Affidavit

The most important document which is submitted in support of a non-consensual interception is the affidavit. The preparation of the affidavit must be supervised by the Assistant United States Attorney who will oversee the interception. Once the affidavit has been completed, it will be reviewed by the AUSA supervising the interception and the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS) if it involves interception of electronics communications. The affidavit will then be forwarded by the CCIPS or the AUSA reviewing the affidavit to Electronics Surveillance Unit (ESU) of the Office of Enforcement Operation (OEO) for review and revision.

The affidavit becomes, in reality, an integral part of the application, outlining the probable cause that has been developed which supports the application for a non-consensual intercept. Although the probable cause standard for a non-consensual intercept affidavit is technically the same as other search and seizure situations, the non-consensual intercept "warrant" is a much more sensitive judicial issue. Therefore, as a

general rule, the highest degree of specificity, consistent with the information available at the time the application is being made should characterize the affidavit. (There should be no tendency to allege only the minimum necessary to establish probable cause.)

Often times, there is a tendency to assert conclusions rather than facts in the affidavit. Therefore, care must be taken to avoid unsupported statements of opinion and conclusions, particularly where they relate to key facts. The source for each item of information in the affidavit should be specified. It is important to set forth underlying circumstances and the factors which give intrinsic reliability to the basic facts established by the affidavit.

The probable cause outlined in the affidavit is expected to be as current as possible. Generally, the Department of Justice expects the basic probable cause to be no more than 15 days old at the time the affidavit, application, and court order are submitted for Department of Justice approval. As is the case in other search and seizure situations, appropriate effort should be made in safeguarding the identity of any intelligence sources which are used for developing probable cause. Particular care should be accorded when establishing the reliability of informants and the accuracy of the information which they provide.

In preparing the affidavit, there are a number of issues which must be addressed and a number of questions which must be answered with specificity. Some of these issues and questions are addressed as follows:

## Details Relating to the Affiant

The following questions must be addressed:

- Is the affiant properly identified? (For joint investigations or task force situations, under the direction of the AUSA, the affiant may be a Secret Service agent or another law enforcement member of the task force or joint investigation).

- Is the affiant's authority as the investigating agent clearly outlined?

- A brief explanation as to the agent's experience with the Secret Service (or other law enforcement member); more specifically, his/her experience with the type of investigation for which the interception is being sought should be included.

## Details Relating to the Target Telephone Number(s)

The paragraph quoted below should always be included in the affidavit in the event the target might change his/her telephone number during the course of a non-consensual intercept. It should be placed just below the paragraph describing the target telephone number in the affidavit.

The **paragraph to be included in the affidavit, application, and, ultimately, in the court order** should read as follows:

> "The authority given is intended to apply not only to the target telephone number listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding post utilized by the target telephone within the 30 day authorization period."

If the interception involves electronic communications (facsimile, Internet or electronic mail), consult the AUSA for the appropriate wording for the affidavit. Once the affidavit has been completed, it will be reviewed by the AUSA supervising the interception and by the Department of Justice Computer Crimes and Intellectual Property Section (CCIPS).

## Details Relative to Previous Application (ELSUR CHECK)

In accordance with 18 U.S.C. 2518(1) (e), the affidavit must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities or locations specified in the application. Electronic Surveillance (ELSUR) checks will be conducted by the Investigative Support Division (ISD), at the request of the case agent. The case agent should contact ISD and provide the names of the potential targets of the interception along with all identifiers available, and all addresses and phone numbers. In joint investigations all participating agencies' indices should be checked by the case agent via their counterpart.

## Details Relating to the Investigation

The following questions must be addressed in the affidavit:

- Are the violations under investigation (specific statute citations), the person (s) to be intercepted, and the facilities or location to be tapped or bugged, clearly identified?
- Have all of the details of the investigation which contribute to the establishment of probable cause been specified?
- Have all sources of information been specified?
- Does the affiant explain the reliability of informants referred to and how these informants obtained their information?
- Is there a "particular description" of the conversations to be intercepted?

18 U.S.C. 2518(1) (b) requires the following:

> **"a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;"**
>
> Note: If any of the persons described who are likely to be intercepted are under indictment or being tried, or if the telephone to be tapped is a public telephone, it should be noted in the affidavit. These circumstances will probably require the court to make certain modifications to the court order. Therefore, their inclusion in the affidavit will alert the court to these situations.

## Details Relating to the Goals of the Investigations

The affidavit must clearly state the goals of the investigation and what results are expected through the use of the interception.

## Details Relating to Investigative Methods Already Utilized

The following questions must be addressed:

- Does the affidavit state with specificity what other investigative methods have been tried and failed, or are too dangerous to try? Included are methods such as the use of standard surveillance techniques, use of undercover agents or informants, execution of search warrants, use of immunity, etc.

18 U.S.C. 2518(1) (c) requires the following:

> **"a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;"**

## Time Period for Interception

The affidavit must specify the period of time requested for the interception. 18 U.S.C. 2518(1) (d) requires the following:

> **"a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;"**

In any event, an initial request for an interception under Title I cannot exceed 30 days. This is specified in 18 U.S.C. 2518(5) as follows:

> **"No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of an extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a**

**provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."**

## Privileged Communications

The following questions must be addressed:

- Does the affidavit outline any expectations that privileged communication will be intercepted?
- If so, does the affidavit, through probable cause, justify such interception?

18 U.S.C. 2517(4) provides that:

**"No otherwise privileged wire, oral or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."**

## Interception of Foreign Languages and/or Code(s)

Information should be provided in the affidavit relating to any use by the target(s) of any codes or foreign languages. If the target(s) of the interception occasionally speak in a foreign language or code, and none of the monitoring agents understand the language, the coded or foreign language portion of such conversations may be monitored and recorded. Later, when a translator or decoding information is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language or code, and the monitoring agent understands the language or code, the entire conversation is subject to the rules of minimization. Additional reference should be made to 18 U.S.C. 2518 (5).

Such information should also be addressed in the preparation of the application and court order.

## 2) Application

After the affidavit has been reviewed and approved by the supervising Assistant United States Attorney, he/she is responsible for the composition of the application.

Although 18 U.S.C. 2510(7) defines the various investigative or law enforcement officers who may technically make application for the interception, it is the policy of the Department of Justice that all such applications be filed with the court by the Assistant United States Attorney who will supervise the interception.

The application is nothing more than an affidavit by the Assistant United States Attorney. It addresses all of the issues which are addressed in the affidavit, albeit in synopsis form. When information from the affidavit is repeated in the application, the same language should be used whenever appropriate, in order to avoid misinterpretation, grammatical error, etc.

The application should specifically reference each supporting affidavit and each affidavit should be made an attachment to the application with these documents attached. If a required statement is inadvertently omitted from the application, this would not necessarily cause the application to be later rejected as an evidentiary document during judicial proceedings. There are a number of issues which are not addressed in the affidavit which must be addressed in the application. They are explained as follows.

## Details Relating to the Applicant

The following questions must be addressed:

- Is the Assistant United States Attorney making the application properly identified?
- Is his/her authority as a law enforcement officer clearly defined?

18 U.S.C. 2518(1) (a) requires that each application include the following:

> **"the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;"**

The Officer authorizing the application is the Attorney General of the United States or his/her designee.

## Details Relative to Previous Application (ELSUR Check)

In accordance with 18 U.S.C. 2518(1) (e) the affidavit must contain a full and complete statement of any prior electronic surveillance (ELSUR) involving the persons, facilities or locations specified in the application. This statement should include the date, jurisdiction, and disposition of any previous applications; as well as their relevance, if any, to the on-going investigation. In addition to any known prior applications, the agency conducting the investigation should conduct an ELSUR check of its own electronic surveillance indices, indices of any other agency participating in this investigation, and the indices of any agency which may have investigated the subjects in the past.

It is only necessary to notify the court of prior applications involving interceptees, premises or facilities named in the present affidavit; persons who have been intercepted on a previous wiretap, but who were not named as interceptees in any court order need not be identified. If such circumstances exist, however, the court should be notified by the AUSA handling the case to avoid a later appellate issue.

## Details of Any Requests for Extensions

Whenever an extension order is being applied for in the application, specific details about results already obtained must be included.

18 U.S.C. 2518(1) (f) requires the following:

> **"where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."**

## Covert Entry

If accomplishment of the proposed interception will require surreptitious or covert entry, the application should so advise the court. This notification will allow the court to modify the court order to allow for covert entry.

## Persons Under Indictment or on Trial

If a probable interceptee is under indictment or on trial, this fact should be noted in the application. This notification will allow the court to modify the court order to allow for interception of this interceptee within prescribed guidelines. These guidelines are described in the COURT ORDER section of this manual chapter.

## Public Telephone Interceptions

If the telephone to be intercepted is a public telephone, this fact should be noted in the application. This notification will allow the court to modify the court order to allow for this kind of interception, within prescribed guidelines. These guidelines are described in the COURT ORDER section of this manual chapter.

## Toll and Subscriber Information

In order to save time during the conduct of the interception, it is recommended that a request for these records be made a part of the application.

## 3) Court Order

After the Assistant United States Attorney has reviewed and approved the affidavit and completed the application, he/she is responsible for the composition of the "warrant" or court order which will be signed by the judge, authorizing the non-consensual interception.

Since much of the information which will be contained in the interception order has been included in the application, the same language should be used whenever appropriate in order to avoid misinterpretation, grammatical error, etc.

## Authority to Issue a Court Order

The authority which allows a judge to authorize a non-consensual intercept order is derived from 18 U.S.C. 2518(3) as follows:

**"Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that -**

**(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;**

**(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;**

**(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;**

**(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire or oral, communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person."**

## Required Information

In preparing the court order, there are a number of issues which must be addressed and a number of questions which must be answered with specificity.

18 U.S.C. 2518(4) requires that the interception order contain the following information:

**"Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify -**

**(a) the identity of the person, if known, whose communications are to be intercepted;**

**(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;**

**(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;**

**(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and**

**(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained."**

18 U.S.C. 2518(4) also provides that, if needed, a court order can be issued compelling cooperation from communications common carriers, landlords, etc., ordering them to **"...furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference...."**

Pursuant to Title 18 U.S.C. 2522, an order may be issued to enforce the assistance capability and capacity requirement under the Communications Assistance for Law Enforcement Act (CALEA)

However, when this type of cooperation is provided for in the court order, efforts must be made to avoid possible breaches of security during the interception. The Department of Justice has concluded that there is no legal need for a communication common carrier, landlord, custodian or other person to be acquainted with the full details of the court order such as, the name(s) of the subject(s) to be intercepted, the violation(s) of law being investigated, etc., in order for them to furnish the necessary assistance. Therefore, in the interest of security, a separate abbreviated court order should be prepared and presented to the court in the applicable circumstances. A copy of this order may be left in the possession of the communication carrier.

## Dates of Implementation and Termination

Court Orders for interceptions are normally for thirty (30) days. Once the court order is signed, a ten (10) day grace period is allowed from the date the court order is signed until the actual interception begins. However, the interception should normally commence as soon as practical after the court order has been signed by the judge. For the actual thirty (30) day operational running time of the wire, and for reporting purposes, the start date is the date the actual interception begins, as long as it is within the ten (10) days after the order was signed.

As is mandated in 18 U.S.C. 2518(4) (e), the court order must contain the period of time for which the interception is authorized.

18 U.S.C. 2518(5) provides specific requirements relative to the dates of implementation and termination as follows:

**"No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communications for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days."**

**"...Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days."**

## Minimization

18 U.S.C. 2518(5) states that the court order shall contain a provision that the authorization to intercept **"...shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter..."**

Minimization is discussed in detail later in this manual chapter.

## Covert Entry

If accomplishment of the interception requires surreptitious or covert entry, this fact should so be stated in both the application and court order. Neither the Electronic Communications Privacy Act of 1986 or the Fourth Amendment require that an interception order include a specific authorization to enter covertly the premises described in the order.

It is, however, the policy of the Department of Justice that such a provision be included in the order authorizing agent/technical personnel to enter the premises surreptitiously; install, maintain, place more effectively, and to remove the interception device at the expiration of the order. Once the initial entry has been accomplished pursuant to the court's order, it is not necessary to secure additional Department of Justice or court approval for subsequent entries in order to accomplish repositioning, maintenance, or removal.

## Persons Under Indictment or on Trial

If a probable interceptee is under indictment or on trial, this fact should be stated in both the application and court order. If this is the case, the interception order should contain restrictive language requiring particular care to avoid the monitoring of conversations pertinent to trial or other disposition of that case. Specific restrictions relative to attorney-client communications are provided later in this chapter.

## Interception of Foreign Languages and/or Codes

The interception of foreign languages and/or codes must also be addressed in the court order. If the target(s) of the interception occasionally speak in a foreign language or code, and none of the monitoring agents understand the language, the coded or foreign language portion of such conversations may be monitored and recorded. Later, when a translator or decoding information is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language or code, and the monitoring agent understands the language or code, the entire conversation is subject to the rules of minimization. Additional reference should be made to 18 USC 2518 (5).

## Details Relating to the Target Telephone Number(s)

The paragraph quoted below should always be included in the affidavit in the event the target might change his/her telephone number during the course of a non-consensual intercept. It should be placed just below the paragraph describing the target telephone number in the affidavit.

The **paragraph to be included in the court order** should read as follows:

> "The authority given is intended to apply not only to the target telephone number listed above, but to any changed telephone number subsequently assigned to the same cable, pair, and binding post utilized by the target telephone within the 30 day authorization period."

## Public Telephone Interceptions

If the telephone to be intercepted is a public telephone, this fact should be stated in both the application and court order. Where a public telephone is to be intercepted, the order should contain a provision to limit, insofar as practicable, monitoring activity to instances when the telephone is being used by those whose interception has been authorized. Physical surveillance of the telephone is usually necessary in this type of situation. Through the use of the surveillance, interception is limited to calls placed by, or to, the subjects.

## Toll and Subscriber Information

In order to save time during the conduct of the interception, it is recommended that a request for these records be made a part of the order. An example of this paragraph follows:

> **IT IS FURTHER ORDERED,** pursuant to 18 U.S.C. 2703 (d), and upon request of the United States, that the _____ Telephone Company of _____ forthwith provide agents of the U. S. Secret Service, subscriber and toll information relative to this order.

## Periodic Reports by the Supervising Attorney

18 U.S.C. 2518(6) provides the following:

> **"Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require."**

The statute does not make the filing of these reports mandatory unless the judge so directs in the authorization order. However, the Department of Justice takes the position that it is clearly in the interest of the Government to file these reports in order to demonstrate continuing judicial supervision over the



interception. Accordingly, the supervising AUSA should, as a matter of course, recommend to the judge that the reporting requirement be included in any order which authorizes the interception of oral communications. The appropriate interval between reports depends upon what is reasonable under the facts of the case. The usual interval, however, is about ten (10) days. The AUSA may call upon the investigative case agent to assist in the preparation of the reports. The format of these reports is usually left to the discretion of the supervising Assistant United States Attorney.

## 4) Authorization Request Letter From the Director or Designee

During this process, the AUSA handling this non-consensual request will be in direct communication with the Department of Justice's Office of Enforcement Operations (OEO). The affidavit, application and court order (draft) will be reviewed and approved by the supervising AUSA and OEO. A copy of each of these documents must be forwarded by the USSS office involved in this application via e-mail, FAX or overnight package delivery service to ISD. Every effort should be made to expedite the submission of these documents, as the probable cause stated in the affidavit must remain current.

Once the documentation has been received, ISD will prepare a letter from the Director's office to the Attorney General, formally requesting authorization to apply for a court ordered interception.

After the formal request letter is prepared, ISD will obtain the signature of the Director or designee. The signed letter, along with the supporting documentation, will then be forwarded to the Electronics Surveillance Unit (ESU), Office of Enforcement Operations (OEO), Criminal Division, Department of Justice. OEO uses this letter as a signal that the Secret Service is in total agreement for the need to conduct this interception.

The following are examples of a formal request letter.

# Sample of Director's Formal Request Letter (Oral communication)

DATE: _____

File Number: _____

Name
Assistant Attorney General
Criminal Division
U.S. Department of Justice

Dear _____,

This letter is submitted in support of an application for a court order authorizing the interception of wire communications on telephone number (___) _____, subscribed in the name of _____, at the address of _____.

Based on information learned from the investigation, we believe the telephone number listed above is being used in connection with violations of Title 18, United States Code, Section _____, and possibly other crimes.

The investigation by this Service shows that the individual(s) identified in the affidavit have been and probably will continue to be involved in violations of the aforementioned sections of the United States Code.

Based on the facts documented in the attached affidavit, the Secret Service believes that the authorization for interception of wire communications will prove fruitful in identifying other co-conspirators, victims, and the manner in which the targets engage in criminal activity.

Sincerely,

_____
Director
United States Secret Service



# Sample of Director's Formal Request Letter (Electronic Communication)

Date: _____

File Number: _____

Name
Assistant Attorney General
Criminal Division
U.S. Department of Justice

Dear _____,

Attached herewith are copies of the affidavit, application, and draft court order prepared in support of an application for a court order authorizing the interception of electronic communications to and from the Internet Protocol address block of xxx.xxx.xxx, with the usable IP address range xxx.xxx.xxx through xxx.xxx.xxx, which presently resolves to a (Name of network or website hosting the IP addresses), located at (address) on the following individuals:

Bob Doe (a/k/a "BDoe"); Jane Doe (a/k/a "Jane"); Roy Jones (a/k/a "RJ"); Peter Parker (a/k/a "Spiderman"), and others yet to be identified.

As the affidavit makes clear, the aforementioned subjects are utilizing a (Name of net work or web site) and are being hosted at (Name of the communication company). There is probable cause to believe that the subjects have committed, are committing, and will continue to commit felony identification document offenses, felony access device offenses, and felony computer crime offenses in violation of Title 18, United States Code Sections _____. Based on the facts documented in the attached affidavit, the Secret Service believes that the authorization for interception of electronic communications will prove fruitful in identifying other co-conspirators, victims, and the manner in which the targets engage in criminal activity.

Sincerely,

_____
Director
United States Secret Service



RIF

## Department of Justice Approval

After the affidavit(s), application and court order have been reviewed by the Office of Enforcement Operations, a recommendation of either approval or rejection will be made to the Deputy Attorney General, Associate Attorney General or a designated Assistant Attorney General. If the request for authorization is approved, the approving official will send a formal approval letter, authorizing the submission of the application for the interception to the United States Attorney in the District where application is to be made. The AUSA supervising the Title I should contact the affiant (the case agent) once the request is approved.

When the letter of approval is received by the AUSA, the case agent will obtain a copy of this letter and will forward the letter to ISD for inclusion in the non-consensual intercept file maintained within the Investigative Support Division (ISD). If the Office of Enforcement Operations rejects the request for authorization, this Service and the supervising AUSA authorizing the application will be notified of the reasons for the rejection and advised of what measures need to be taken in order to reapply for the interception.

## Headquarters Team Assistance

After the application is submitted to Headquarters, and pending approval from DOJ Office of Enforcement Operations, a team comprised of the following personnel will travel to the field office involved to coordinate the administrative requirements and future conduct of the interception:

**Representatives from the Investigative Support Division (ISD)** will meet with the supervisory agents and the case agent of the office handling the interception concerning the manual requirements, minimization, and wire room restrictions for the interception operation. If requested, ISD will assist the case agent in preparing his or her portion of the briefing for the interception.

**Representatives from the appropriate operational division** will be responsible for meeting with the SAIC, case agent and the Assistant United States Attorney, as necessary, to go over any questions raised during the review of the affidavits, application, and court order. They will also meet with the case agent and office supervisory personnel to identify and resolve surveillance and wire room manpower requirements, costs, and other case related issues.

**Representatives from the Technical Security Division (TSD)** will coordinate with the local telephone company to review the technical aspects of the interception. TSD will determine a suitable site and additional equipment requirements. The type of intercept will dictate the equipment needs (i.e. phone, cellular phone, fax, e-mail).

This team assists the case agent in the details of planning the intercept and bringing to the site the necessary personnel and equipment without the case agent specifically requesting them.

After the Department of Justice has approved the interception and the court order is expected to be signed, this team may travel again to the office to assist in setting up the wire room and attend the minimization briefing given by the AUSA. The case agent needs to prepare the case briefing, specific agent assignments, and administrative data (scheduling, hotel information, etc.).

The minimization briefing must be attended by all interception personnel, including surveillance agents and field office administrative support. If wire room personnel must be replaced after the briefing due to exigent circumstances, the replacements must receive a similar briefing.

Once the wire room personnel have been briefed and are confident that all procedures and the conduct of the intercept comply with DOJ and Secret Service policy, the ISD representatives will return to Washington, DC.

ISD representatives will continue to monitor the progress of the intercept and be available to answer questions and give advice to the case agent and the wire room supervisor. If necessary, the ISD representatives can return to provide on-site assistance.

## Application to the Court

After the Department of Justice has formally approved the application for authorization of the interception, the supervising Assistant United States Attorney will submit the application to a judge having jurisdiction within the district where the interception is to take place. The application should be presented as expeditiously as possible following the receipt of authorization.

Although interception orders may be granted by judges of a United States District Court or judges of the United States Courts of Appeals, the Department of Justice mandates that, except in extraordinary circumstances, all applications should be presented to a District Court Judge. The documents to be presented to the judge include the originals and one (I) copy each of the affidavit(s), application(s), court order(s) (draft), and Department of Justice authorization letter.

## Sealing of Documents

If a court order is granted, the court or the supervising Assistant United States Attorney, in the court's presence, will seal the court order along with all related documents. The usual practice is either to file the sealed package with the District Court Clerk for safekeeping in the clerk's vault, or for the supervising Assistant United States Attorney to retain custody of the sealed documents until the interception has been completed, at which time they will be filed with the court.

A copy of the documents may be kept by the supervising Assistant United States Attorney. Each district may vary as to "sealing" procedures. Questions as to the proper procedure should be directed to the appropriate official in the U. S. District Court Clerk's office.

## Procedure if the Application for an Interception Order is Denied

If the court refuses to issue an interception order, the appropriate Assistant Director's office must immediately be notified of the reasons for this rejection. The supervising Assistant United States Attorney will immediately notify the Office of Enforcement Operations. That office will determine whether a new application can or should be made based on the facts immediately available, or whether additional investigation is needed.

# Emergency Interceptions

18 U.S.C. 2518(7) provides for the interception of communications for up to 48 hours, without a prior court order, under certain emergency conditions. However, that section also provides that an application for a court order approving the interception must be made within 48 hours after the interception has begun.

The Attorney General, Deputy Attorney General, and Associate Attorney General all have the power to authorize emergency interceptions. This emergency provision does not dispense with any of the application procedures prescribed under 18 U.S. C. 2518(1). It merely delays the application process for 48 hours. The Director or his/her designee must obtain oral authorization and submit a written request for the emergency interception. This request must identify the persons to be intercepted, the facilities from which, or the place where, the wire or oral communications are to be intercepted, and the offenses that are expected to be related to these interceptions.

Furthermore, 18 U.S.C. 2518(7) requires that the request letter specifically explain the justification for an emergency interception. 18 U.S.C. 2518(7) (a) clearly sets forth the definition of an "emergency situation" that will warrant an interception without first obtaining a court order. Emergency situations include those which involve conspiratorial activities which threaten the national security interest or which are characteristic of organized crime or any offense that involves immediate danger of death or serious physical injury.

The request should be accompanied by documentation setting forth probable cause that:

(1) An individual is committing, has committed, or is about to commit a particular offense enumerated in 18 U.S.C. 2516;

(2) That particular communications concerning the offense cited will be obtained through such interception;

(3) That the facilities from which, or the place where, the wire or oral communications are to be intercepted, are being used, or are about to be used, in connection with the commission of such offense.

Explicit guidelines for the conduct of an emergency interception are set forth in 18 U.S.C. 2518(7). Whenever an emergency interception is being contemplated, the Assistant United States Attorney who would supervise such an interception should immediately contact the Office of Enforcement Operations (OEO) for guidance and advice. In practice, the emergency procedures are initiated when the AUSA in charge of the case contacts an Electronic Surveillance Unit (ESU) attorney at OEO. At the same time, the case agent should contact the Investigative Support Division (ISD) and the appropriate operational division. After discussions with the AUSA, the ESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements for the emergency interception have been met. Once approved, the ESU attorney notifies the AUSA supervising the case.

The Director or his/her designee (OEO) then contacts the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AAG) to seek permission and to make a determination that an emergency situation exists as defined in the statute.

# Preparing to Conduct the Interception

After a judge has issued the interception "warrant", 18 U.S.C. 2518(5) requires that the authorization to intercept be executed as soon as practicable. If all of the preparatory procedures which have thus far been

outlined in this chapter have been followed, execution of the interception "warrant" can begin as soon as it is issued.

Prior to conducting any interception, all Secret Service employees and other law enforcement personnel participating in the interception must read and understand this chapter, minimization memorandum, affidavit, application and court order. The guidelines contained in this chapter have been designed to assure strict adherence to the laws and procedures which govern the use of these interceptions.

**It is the philosophy of the Secret Service that it is preferable to err on the side of caution rather than risk any inadvertent violation of law or established procedure when conducting these interceptions.**

# Staffing Requirements

Non-consensual interceptions are sensitive in nature, and, as such, require great care in their execution. The USSS field supervisor overseeing the interception should insure that staffing is properly allocated and utilized during the operation. Staffing may include personnel from other law enforcement agencies who are task force or joint investigation participants. Whenever possible, eight hour shifts should be utilized during the operation. However, twelve hour shifts may be acceptable depending on the volume of calls and activity anticipated and the availability of manpower.

## Supervising Agent

The Supervising Agent ("Wire Room Supervisor") normally is the liaison between the supervising Assistant United States Attorney (AUSA) and the monitoring agents. This insures that instructions from the AUSA are properly communicated to the monitoring agents and that the supervising attorney receives an accurate overview of what the interception is producing.

The Supervising Agent is also charged with the responsibility of conducting the interception in compliance with all instructions of the court and the supervising AUSA and insuring that the interception devices are installed as soon as practical after the court order is obtained.

The Supervising Agent will also insure that information gained from the interception is communicated, in a timely manner, to the case agent and surveillance personnel.

The Supervising Agent will be responsible for the chairing of daily meetings involving key interception personnel, providing timely distribution of information and updating operational instructions.

The Supervising Agent should prepare and deliver to the supervising AUSA daily written reports. Copies of these reports should be made for the case agent. There is no prescribed format for such reports, but they should show the nature and scope of the interception for that day. For instance, they should indicate the number of pertinent (relevant) conversations intercepted, the number of non-pertinent conversations minimized, whether any of the targets named in the order were intercepted, whether any new targets were identified, and whether any problems have arisen( e.g. equipment malfunction, privileged communications, or evidence of other crimes).



These daily reports should be made even throughout a weekend or holiday period and may initially be accomplished via telephone with the documentation being prepared the next working day. A copy of the corresponding day's consecutive call log should accompany each report. The Supervising Agent's duties include providing for the overall integrity of the interception as well as the integrity and admissibility of the evidence obtained by following the principles and guidelines set forth within this manual.

The Supervising Agent should insure that the interception is properly terminated at the time specified in the court order, or when the objective of the interception has been accomplished, whichever comes first. The Supervising Agent is responsible for the operation and will coordinate all external surveillance activity with the surveilling agents. It is important that he/she have an overview of the entire investigation and be able to confirm voice identifications, identify patterns of involvement and generally maximize the effectiveness of the interception.

Since the Supervising Agent's primary purpose is to insure the integrity of the interception operation, he/she will not be the case agent for the investigation for which the interception is conducted. (The case agent cannot properly devote the time and attention required during the execution of the interception.) Whenever possible, only one Supervising Agent should be assigned to the interception. However, more than one may be assigned during very active interception operations.

## Wire Room Shift Leader

The Wire Room Shift Leader will be a senior Special Agent who is familiar with the entire investigation. He/she will supervise wire room activities, monitor personnel, and ensure the integrity and security of the wire room during their particular tour of duty. The Shift Leader will maintain liaison with the Supervising Agent and TSD support personnel, who will maintain the integrity of the equipment under their supervision. In the absence of a Supervising Agent (i.e. midnight shift), the Shift Leader will assume the responsibilities of the Supervising Agent in notifying the supervising AUSA, case agent and surveillance personnel of relevant information when necessary. The Shift Leader will keep the monitoring personnel appraised of any significant developments in the case that may affect the monitoring of the interception.

## Monitoring/Minimization Personnel

The personnel (normally Special Agents) assigned to the actual interception, monitoring, and recording of conversations are in the most sensitive position of the interception operation. They must adhere carefully to the minimization guidelines set forth in the court order and by the supervising AUSA. The monitoring personnel must be accurate in the recording of all information in the Consecutive Call Log which they will maintain. They are not to discuss the content or context of any of the calls monitored with any individual (including agents or other personnel) who do not have a **specific need to know**.

Prior to assuming their monitoring duties, all monitoring personnel must listen to any recordings made earlier during the investigation in order to familiarize themselves with the voices of the targets intercepted during those conversations. Separate monitoring personnel must be assigned to each target telephone line; if any target telephone line is deemed to be extremely busy, then two people should be assigned to monitor that line.

In the case of interception of electronic communications, monitoring personnel requirements vary depending on number of Internet Protocol (IP) addresses intercepted. However, one minimization employee should be assigned per one Internet Protocol (IP) address. See the Interception of Electronic Communication section of this chapter for additional information, page 44).

## Technical Security Division (TSD) Personnel

In most cases, Technical Security Division (TSD) personnel will be responsible for obtaining the necessary technical information and equipment needed to accomplish the interception. TSD will also secure and establish the monitoring area in conjunction with the Supervising Agent and Shift Leader(s).

The only persons who are authorized to install and test interception and recording equipment are TSD specialists (Telecommunication and Security Specialist, or Special Agent). TSD personnel will be readily available at any time during the interception in order to respond to technical problems which may arise.

In the case of interception of electronic communications, ECSAP trained Special Agents may install, maintain and test interception and recording equipment in coordination with the TSD personnel.

In addition, TSD will make all necessary coordination with the telephone or internet service provider and equipment manufacturers to obtain necessary equipment for telephone (hard line and wireless) and electronic communication interception. The most up to date telecommunication interception equipment available and capable of intercepting oral communication and call data will be installed on all anticipated target telephone lines.

The TSD representative should coordinate his/her activities with the case agent or other designated agent personnel to provide the necessary information for the issuance of judiciary subpoenas requesting subscriber and other telephone information.

To preclude obtaining a subpoena each and every time subscriber information, or other information, is needed from the telephone company; the court in the original non-consensual interception order can direct the telephone company to provide this information as needed by this Service.

**TSD personnel should never be used for monitoring, nor should they be used for any other function normally assigned to a Special Agent.**

## Criminal Research Specialists (CRS) and Data Analysis

CRS personnel from ISD will be assigned to accomplish the required database searches and telephone toll link analysis as necessary using analytical software.

The number of CRS personnel assigned to the interception will depend on the volume of calls and activity anticipated during the interception. However, in most cases, it may be appropriate to assign at least one CRS who has been trained in the call data and telephone toll link analysis requirements and capabilities of PenLink, as well as other computer programs. Prior to the initiation of the interception, vital aspects of these applications will be discussed with the Wire Room Supervisor and case agent in accordance with the U.S. Secret Service guidelines for standardization of software.

For utilization of CRS support in an interception the SAIC - ISD must be contacted. For specific information regarding the Criminal Research Specialist Program, see the Investigative Manual, ISD-19.

## Transcribing Personnel

One of the most critical elements of the interception is the transcription of intercepted conversations. In order to effectively transcribe these conversations, the transcribers should have a thorough knowledge of the investigation, the targets involved, and the violations of law under investigation. Administrative support personnel may be used to type the transcribed conversations, but agent personnel must thoroughly review the transcription.

In cases where intercepted conversations are conducted in a foreign language, language specialists from other agencies or approved private contractors may be used to aid in monitoring the calls and transcribing them into English.

The amount of transcription during the interception will depend on the guidelines set forth by the supervising AUSA and the needs of the supervisory and case agents.

## Surveillance Personnel

Whenever possible, visual surveillance should be conducted in conjunction with the interception. Incriminating conversations, obtained from the interception, will have a greater impact during presentation at trial if it is corroborated by testimony from surveillance agents, or joint investigation/task force members, confirming that the target(s) were at a certain location or attended a certain meeting when an interception was made.

Surveillances conducted in conjunction with the interception will often provide a better overview of the target's involvement in the violation of law under investigation and may provide additional probable cause for court ordered extensions of interceptions. The use of surveillances may develop very valuable investigative leads and advance knowledge of target actions.

The number of surveillance agents required during the interception operation will depend on the number of targets involved, the number of target telephones, the violations of law under investigation, etc. In any case, the use of surveillance agents requires close communication and liaison with the Supervising Agent (Wire Room Supervisor) and the case agent.

## Other Investigative Tactics

In an ideal situation, pertinent conversations will be intercepted as soon as the interception operation begins. However, in many cases extensive monitoring takes place before pertinent and/or incriminating conversations are recorded. In these situations, it may be possible to induce the targets to discuss the violation of law under investigation.

These inducements can be accomplished in a number of ways. If the investigation involves the use of an undercover agent or confidential informant, the agent or informant may be used to generate conversations between targets by placing calls to these targets, thereby making inquiries about the illegal activity under investigation. The undercover agent or confidential informant may very well be in a position to place "orders" for contraband, thereby inducing the targets to engage in incriminating conversations.

Interviews of targets, or friends or associates of targets, conducted by agents may also induce conversations between the targets. If the targets believe that arrests are imminent, or that inquiries are being made about the violations of law under investigation, these targets may very well participate in pertinent and/or incriminating conversations.

The innovative investigator can utilize a myriad of investigative tactics designed to maximize the effectiveness of the interception, and this innovation is certainly encouraged. However, before any of these tactics are employed, their use should be approved by the supervising AUSA, and closely coordinated with the supervising agent and case agent.

## Field Office Wire Room

In most cases, and whenever possible, the interception operation will be established within a field office through acquisition of a leased (dedicated) telephone line(s) which is connected to the circuit utilized by the target telephone(s). The Investigative Support Branch of TSD should be consulted to ensure the most cost effective method of line installation.

The interception and recording equipment must be installed and secured within a room in the field office which can be separately secured and which will not be accessed by personnel who are not directly involved with the interception operation. As soon as the monitoring station is capable of becoming operational, i. e., the leased line(s) have been installed and is active and the interception and recording equipment is on site, the monitoring station should be considered secure and accessible to only authorized personnel who are directly involved with the interception.

At this time, a Personnel Access Log (SSF 3285A) must be posted and maintained at the entrance to the monitoring station. All persons who access the wire room must make the appropriate entries in the log each and every time they enter or exit. The Supervising Agent and/or Shift Leader have the responsibility to ensure that these procedures are adhered to by all personnel.

> **Note:** Should the wire room be protected by an electronic access system, the use of the Personnel Access Log can be suspended in lieu of a computerized printout.

The Personnel Access Log (SSF 3285A) can be found via the USSS Forms Library at Intranet address http://ssweb/mno/pars/forms.

## Outside Wire Room

If circumstances prevent establishing a wire room within a field office, it is necessary to obtain a suitable site at an outside location. Twenty-four (24) hour security coverage will be placed on the wire room as soon as it is capable of becoming operational, i.e., the leased lines has been installed and is active and the interception and recording equipment is on site. At this time, the personnel operating the wire room will begin to maintain a "Personnel Access Log."

If the location of the wire room normally allows access by "outside" personnel (hotel room maids, etc.), arrangements should be made to deny them access to the wire room.



# Conducting the Interception

## Monitoring and Recording

The law makes no distinction between "listening to", "monitoring," or "recording" a conversation. Courts generally regard an interception order in the same light as any other warrant; it authorizes a limited "search" and limited "seizure" of evidence. Whether a conversation is merely overheard, or if it has been recorded, makes no difference legally; it has been seized.

## Minimization

One of the most critical issues relative to a court ordered interception pursuant to Title I is the issue of minimization. 18 U.S.C. 2518(5) requires that every court ordered interception must "contain a provision that the authorization to intercept...shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception..." This provision requires that the interception procedures be conducted in such a way so as to include the smallest possible number of interceptions of "innocent" communications.

In this context, the word "possible" means feasible or practicable consistent with the objective of obtaining evidence of the criminal activity described in the interception order. In a normal situation, some interception must take place before it can be determined that the interception of the communication should be interrupted. It is difficult to establish set rules in this area, for there appears to be an exception to every truism concerning minimization.

As a guiding principle, problems relating to minimization must be dealt with on an ad hoc basis, and monitoring personnel must be provided with instructions by the supervising AUSA as the interception operation progresses. The minimization process should be monitored closely by the Wire Room Shift Leader to ensure continuity. The character of the criminal enterprise, i.e., the nature of the activity, its complexity and size, its geographical reach, and similar considerations all bear on the conduct of an interception.

The purpose of the investigation may be a critical factor in determining the authorized scope of the interception. Where an objective of the interception is to define the scope of criminal activity, or to identify unknown conspirators, or to obtain information on the operation of an illegal enterprise, the parameters of interception are much broader than when an interception is instituted for a narrow, limited purpose.

If, however, the expected content of the communications to be intercepted is narrow in scope, efforts should be made to minimize accordingly. For example, if, at the time of the initiation of the interception, the monitoring personnel know all the targets who are suspected of the criminal offense, they can tailor their minimization efforts to avoid monitoring incoming or outgoing calls involving other persons. Similarly, if the monitoring personnel know during what time of day the telephone will be used for criminal activity, they can avoid intercepting calls at other times.

Such considerations affect the initial minimization tactics employed during the investigation, but the interception policy may be changed to conform with investigative requirements as the interception continues. On the other hand, where the monitoring agents do not, at the outset, have reason to believe that any identifiable group of calls will be innocent, it may be reasonable to monitor all calls until a pattern of innocent



calls develops. Such a pattern may not always be identifiable because it is often impossible to determine that a particular conversation would be irrelevant and innocent until it has been concluded.

The use of code words, cover-up jargon, or other evasive tactics makes investigation difficult and necessitates more detailed and extensive monitoring of conversations. Accordingly, the interception of all telephone communications for such time as is appropriate where evasive tactics are used does not constitute a failure to minimize.

In analyzing the overall interception, the courts have said that telephone conversations of brief duration do not permit monitoring personnel sufficient opportunity to identify the caller and characterize the conversation. Interceptions of conversations completed in less than two (2) minutes cannot be considered unreasonable. Moreover, calls between known co-conspirators may be monitored in their entirety since relevant information may emerge at any point in a call.

Where one of the parties is a known conspirator, the monitoring of his/her conversations may be more extensive than if he/she were not suspected, at least during the early phases of the interception; by listening to such calls, monitoring personnel can effect the screening of unknown parties. The interception of communications of suspected conspirators is similarly appropriate until their complicity can be determined.

The courts have endorsed a variety of methods which may be employed when attempting to "minimize" interceptions. The methods which would most likely be employed by this Service fall into three categories: **extrinsic, intrinsic and after-the-fact** minimization. Each approach to minimization involves different procedures; however, more than one approach may be employed during an interception operation.

## Extrinsic Minimization

Extrinsic minimization involves limiting the time period during which monitoring is conducted. Although a judge may issue a non-consensual interception order for an effective period of up to thirty days, most orders are effective for only fifteen or twenty days. This is one example of extrinsic minimization.

A second example of extrinsic minimization is the termination of interceptions before the expiration of the court order. A third example would be a situation where monitoring is restricted to certain hours each day, depending on the type of violations involved and the circumstances in the case.

## intrinsic Minimization (Spot Monitoring)

Intrinsic minimization (or "spot monitoring") is the most common method of minimization used during voice interceptions. It involves the screening of all conversations as they are taking place. This method requires the monitoring personnel to make a reasonable, good-faith effort to avoid either listening to or recording non-pertinent conversations.

Monitoring personnel must be permitted a reasonable amount of flexibility to guard against the possibility that a conversation which appears non-pertinent at first may later become pertinent, involving discussions of violations cited within the court order. Spot monitoring is a method which provides the monitoring agents with this flexibility.

If the monitoring personnel listen to the first part of a conversation and cannot determine with certainty that it is either pertinent or non-pertinent, the monitor should deactivate the listening and recording devices. Periodically thereafter, the monitor should reactivate the listening and recording devices for brief periods until the nature of the conversation and/or the identity of the subject can be verified.

## After-the-Fact Minimization

After-the-fact minimization for an audio interception involves recording every conversation and then restricting disclosure of non-pertinent conversations by transcribing or re-recording only pertinent conversations and then sealing the original tapes. Except under extraordinary circumstances, and then under the strict supervision of the supervising AUSA, this method of minimization for an audio intercept will not be employed by this Service. (Foreign language minimization is covered in the section below.)

In the instance of interception of electronic communications (fax, internet, e-mail, and online instant chat), after-the-fact minimization has to be the method utilized. This will involve intercepting and reading all of the fax or email transmissions and then determining which are pertinent or non-pertinent. The supervising AUSA will provide guidance when using this type of minimization.

## Foreign Languages

If the targets of the interception occasionally speak in a foreign language, and none of the monitoring personnel understand the language, the foreign language portion of such conversations may be monitored and recorded. Later, when a translator is available, the conversations can be minimized (after-the-fact minimization). However, if most of the conversation is in a foreign language, and monitoring personnel understand the language, the entire conversation is subject to the rules of minimization. Seek the guidance of the supervising AUSA when using this type of after-the-fact minimization.

## Public Telephones

If the target telephone is accessible to the general public, as well as to the targets of the interception, the monitoring personnel must avoid interceptions of individuals who are not included in the court order, i.e., members of the general public. This can most easily be accomplished through a visual surveillance of the target telephone. The surveillance personnel can notify monitoring personnel when a target utilizes the target telephone.

If surveillance cannot be accomplished, the monitoring personnel should monitor conversations only when the voices are recognized as those of the targets or suspects or when the dialed telephone numbers are recognized as suspect.

## Evidence of Other Crimes

If the monitoring personnel overhear conversations which apparently relate to crimes which are not enumerated in the court order, they should continue to intercept and record this type of call as though these crimes were included in the court order. However, these newly developed crimes and the interceptions relating to them should be reported to the supervising AUSA as soon as possible, but not later than the next day.

The supervising AUSA will then make a determination as to whether the intercepted conversations may be evidence of a crime not listed in the court order. If so, the supervising judge will be informed by the supervising AUSA.

## New Targets

One of the stated and authorized purposes of the interception is to identify additional targets in the investigation who have not been named in the court order. Whenever any such individual is identified by name, nickname, telephone number, etc., the supervising AUSA should be notified immediately. He will then notify the court and a determination will be made as to whether or not an amendment to the court order is required.

## Privileged Communications

One of the primary objectives of authorized interceptions of private communications is to provide the investigative agency with legally admissible evidence of criminal activity which could not be obtained through normal investigative techniques. However, the confidentiality of conversations between individuals who stand in the relationship of husband - wife, clergyman - parishioner, physician - patient, and attorney - client are protected by testimonial privilege.

Accordingly, 18 U.S.C. 2517(4) states as follows:

> **"No otherwise privileged wire, oral or electronic communications intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."**

If an intercepted communication would be otherwise privileged, it cannot be introduced as evidence. Whenever monitoring personnel become aware that the conversation being monitored is privileged, they should immediately deactivate the listening and recording devices and, as soon as practicable, notify the Wire Room Shift Leader and the supervising AUSA of the interception.

Whenever privileged communications are partially intercepted, the monitoring personnel must indicate this fact in the Consecutive Call Log. A more serious situation is presented when the conversations overheard by monitoring personnel are between the target and his/her attorney (or vice versa). In this instance, the confidential communication is not only protected by a testimonial privilege, but also by the Sixth Amendment's guarantee of the individual's right to the assistance of counsel.

If the intercepted communications deal with legal advice given by the attorney to the client concerning a pending criminal case, then care must be taken not to violate the client's Sixth Amendment rights. In the event that monitoring personnel intercept a communication between an attorney and client concerning a pending criminal case (i.e., a case in which the client is under indictment). the monitoring personnel must immediately deactivate the monitoring and recording equipment and make a notation in the Consecutive Call Log that the conversation was partially intercepted and was not completely overheard. The entries in the log should identify the attorney and the client who were intercepted.

In rare instances, this Service may be authorized to intercept the conversations of a target and his/her attorney after an indictment has been returned against the target. However, great care must be exercised by the supervising AUSA that pending cases against a target are not needlessly jeopardized in order to further potential cases.

In the event the electronic surveillance intercepts a communication between an attorney and client relating to matters other than a pending criminal case (e.g., a conversation in relation to an illegal activity), the monitoring personnel should, at the earliest practicable moment, bring this fact to the attention of the Wire Room Supervisor and the supervising AUSA. Upon being informed of the circumstances and content of the conversation, the supervising AUSA must decide if the conversation is, in fact, privileged.

If that determination is made, the supervising AUSA should instruct this Service not to disclose the content of the privileged communication to other investigative or police agencies, or conduct further investigation based upon the contents of the privileged communication. Such privileged conversations should not be included in the copies of transcriptions of the tapes, but should be recorded on the sealed copy that will remain in the custody of the court.

## Minimization Memorandum

The issue of minimization is one of the most critical issues relative to a court ordered interception conducted under Title I. For this reason, Secret Service policy requires that all personnel, who are to be responsible in any way for the conduct of the interception, read and initial a memorandum which outlines the issues involved with minimization prior to conducting the interception. In most cases, this memorandum will be authored by the supervising AUSA; if, however, the supervising AUSA is not the author, it will be the responsibility of the Supervising Agent to author the memorandum.

In addition to reading this minimization memorandum, all interception personnel will be responsible for reading the court order, application, and affidavit supporting the interception.

The following pages contain a sample minimization memorandum which addresses all of the issues that must be understood by all participating personnel prior to conducting the interception. **Note:** An after-the-fact minimization memorandum may differ in content at the discretion of the AUSA.

## Sample of Minimization Memorandum

MEMORANDUM

DATE: _____

FROM: _____

United States Attorney
By: _____
Assistant United States Attorney

SUBJECT: Minimization of Interceptions

TO: All Supervisory and Monitoring Agents and other personnel of the U.S. Secret Service Participating in the Interception of Wire Communications, to and from Telephone Number(s)

**IMPORTANT**: This memorandum and the attached court order, application, and affidavit **must** be posted within the listening post and said items shall be read in their entirety by all supervisory and monitoring agents participating in any interception **prior** to such participation. The attached Review Log **must** be signed and dated acknowledging same. YOU MUST NOT PARTICIPATE IN ANY MONITORING UNTIL ALL OF THE ABOVE LISTED ITEMS HAVE BEEN READ AND UNTIL YOU ARE TOTALLY FAMILIAR WITH THE FEDERAL VIOLATIONS ENUMERATED IN THE COURT ORDER.

Your objective is to execute the court order, recording only those conversations which are specifically designated, and minimizing the interception of non-pertinent or privileged communications.

**I. LEGALLY THERE IS NO DIFFERENCE BETWEEN "MONITORING" AND "RECORDING"**

The law makes no distinction between "LISTENING," "MONITORING," or "RECORDING" a conversation. Courts generally regard a wire interception like any other search warrant: it authorizes a limited "search," and limited "seizure" of evidence. Whether a conversation is merely overheard or also recorded makes no difference legally; it has been seized.

If you "seize" everything that is intercepted, the fruits of your investigation are likely to be suppressed. We have to establish that we neither LISTENED to **nor** RECORDED conversations we had no right to overhear. We have to establish that we are making and have made a reasonable effort to stay within the legal limits of the court order.

# Sample of Minimization Memorandum (page 2)

**II. CONVERSATIONS WHICH MAY BE LISTENED TO**

We have authority to intercept telephone conversations of _____ a/k/a _____ and _____ (list all targets) and others yet unknown concerning violations of Title 18, United States Code, Sections _____ and _____. (List all violations cited in court order). Any interception of a non-enumerated offense must be brought to my attention (supervising Assistant United States Attorney) through the Supervising Agent immediately.

Listen to the beginning of each conversation for only a period of time as is necessary to determine the parties and the nature of the conversation; if the parties or the nature of the conversation are not covered by the order, TURN OFF THE LISTENING AND RECORDING DEVICES.

If the targets act with great circumspection, i.e., coded, guarded, or cryptic language is used, the monitoring agents may be justified in monitoring a significant part, or perhaps all, of a conversation in order to be sure that it is indeed innocent.

**III. NEW TARGETS**

One of the stated and authorized purposes of the interception is to identify additional targets in the investigation who may have not been named in the court order.

Whenever any such individual is identified by name, nickname, telephone number, etc., I (supervising attorney) should be notified immediately. I will then notify the court and a determination will be made as to whether or not an amendment to the court order is required.

**IV. CONVERSATIONS WHICH MAY NOT BE LISTENED TO AND RECORDED**

The court order is quite clear that we must not listen to any "privileged" conversations, and must minimize the interception of conversations which do not relate to the criminal activity under investigation.

**V. PRIVILEGED COMMUNICATIONS**

We must not listen to any conversation which would fall under any legal privilege. The general categories of privileged communications are as follows: Attorney - Client; Clergyman – Parishioner; Doctor -Patient; Husband - Wife.

**A. ATTORNEY - CLIENT:**

Consider this an absolute rule: **NEVER** knowingly listen to or record a conversation between a target and his attorney.

Should there be any conversations between any of the targets and any of their attorneys, you are**NEVER** to listen to **ANY** portion of **ANY** of these conversations at **ANY** time. To listen to any conversation with any of these attorneys could result in the dismissal of a pending indictment. If you should listen to a conversation with an unknown individual, and you determine that this individual is an agent or an employee of one of these attorneys, you should instantly cease monitoring the conversation. If you happen to accidentally monitor a conversation with one of these attorneys or their agents or employees, make a note of that conversation and its contents, immediately notify me, but until given further instructions DO NOT relate to anyone the substance of that conversation (this includes any other agent of the USSS).

If at any time during the investigation we learn of the name(s) and/or telephone number(s) of any attorneys retained by our targets, this name and telephone number are to be posted in a conspicuous place in the monitoring site. Any dial-outs to that telephone number require that the recorder and monitoring device be turned off as soon as it is ascertained that it is an attorney who is calling our subject or being called by him/her.

**B. PARISHIONER - CLERGYMAN:**

All conversations between a parishioner and his clergyman are to be considered privileged. We could not obtain an interception warrant to listen to a man confess his sins to a priest in a confessional booth; similarly, we must not listen to a target discuss his or her personal, financial or legal problems with his or her priest, minister, rabbi, etc.

**C. DOCTOR - PATIENT:**

Any conversations a patient has with a doctor relative to diagnosis, symptoms, treatment, or any other aspect of physical, mental or emotional health is privileged. The instant it is learned that one of our targets is talking to a doctor about his or her health (or someone else's health), TURN OFF THE MACHINE. STOP LISTENING. STOP RECORDING.



RIF

# Sample of Minimization Memorandum (page 3)

D. **HUSBAND - WIFE:**

Any conversation between a husband and his wife which relates in any way to the marital relationship is privileged. For example:

If they discuss their sex life - DON'T LISTEN. DON'T RECORD.

If they discuss problems their child is having in school - DON'T LISTEN. DON'T RECORD.

If they discuss a fight or argument they had a night or day or week ago - DON'T LISTEN. DON'T RECORD.

However, it may be that a target's wife or husband acts as a partner, message taker or message-deliverer for a target. Therefore a limited degree of spot monitoring may be conducted if a target calls his or her spouse. (See Section VII B, below.) If a pattern develops demonstrating that our target's spouse is in fact deeply involved in the target's dealings, then further monitoring as with any newly identified co-conspirator may be in order. However, the matter must be reported by me to the Court, so that an amendment to the court order can be made, adding the spouse as a target.

E. **OTHER RELATIONSHIPS**

No legal privilege exists with regard to conversations between any of the targets and his or her paramour.

Similarly, no legal privilege exits with regard to conversations between any of the targets and their children.

However, keep in mind that our function is to intercept and record conversations related to violations of specific Federal statutes, not to indiscriminately invade the privacy of our targets and others.

In general, follow the rules outlined in paragraphs VI and VII.

VI. **"MINIMIZATION"**

It is hereby ordered, that the execution of this order shall be conducted in such a way as to minimize the interception of communications not related to the violations of law under investigation. Your job is to listen to/record all pertinent conversations, while minimizing the interception of innocent (non-criminal) conversations.

That is easy to say, and difficult to do. We cannot expect the targets to oblige us by using words which specifically indicate their criminal activity. Codes, vague expressions, oblique references are quite likely to occur during monitoring.

Therefore, it may be necessary to listen to and record some non privileged conversations which in fact do not relate to the violations of law under investigation.

In my opinion, the courts will not suppress pertinent conversations simply because some non-privileged and non-pertinent conversations have been intercepted.

Always remember, however, that eventually a court may have to decide whether we executed the interception in a manner specified by the court order.

The standard which a court is likely to apply, in determining whether there was an overly broad listening to non-pertinent conversations, is simply:

Did the officers make a reasonable effort to comply with the restrictions and requirements of the court order?

"...a court should not admit evidence derived from an electronic surveillance order unless, after reviewing the monitoring log and hearing the testimony of monitoring agents, it is left with the conviction that on the whole the agents have shown high regard for the right of privacy and have done all they reasonably could to avoid unnecessary intrusion." **U.S. v. TORTORELO**

"...the monitoring agent and thereafter the reviewing court must consider many factors, including the precise relationship of the parties, the length of the relationship, the number of calls between the parties, the state of the investigation, activities... of the alleged conspirator who is a party to the conversation, and the content of the conversation to determine the appropriate degree of minimization."**U.S. v. FALCONE**

# Sample of Minimization Memorandum (page 4)

The Supreme Court has announced a standard for minimization which requires that interceptions be **objectively** reasonable in view of both the purpose of the investigation and the **facts** available to the monitoring agents at the time of the interception.

It is, therefore, important for each monitoring agent to be familiar with the factual background in this case in order that, if necessary, he may be prepared to articulate the reasons for the frequency and duration of any given interception in which he participated.

Keep in mind that each of you may be required to explain from the witness stand why a particular conversation was intercepted.

Make a good-faith effort to comply with the central purpose of the interception warrant: to intercept and record conversations pertaining to the conspiracy under investigation. Use your common sense. Make a good-faith effort to comply with the purposes and restrictions of the interception warrant. I can't expect anything more from you, and neither, in my opinion, will the courts.

VII. **SPOT MONITORING OR SPOT CHECKING**

Assuming that a conversation does not, during the first two minutes, fall within the scope specified within the court order, the interception and recording devices must be turned off. However, it is possible that some time after the interception and recording devices have been turned off, a target may get on the telephone or the parties might begin to engage in conversations that relate to the violations of federal law which are set forth in the court order. To guard against missing such a conversation, listen periodically (spot monitor) by activating the interception and recording devices every 30 to 60 seconds or so to determine if the parties or nature of the conversation have changed to within the scope specified within the court order. LISTEN FOR A FEW SECONDS. If during this brief listening period, it appears that the conversation falls within the scope of the court order, continue to listen and record. If there is no such evidence, TURN OFF THE INTERCEPTION AND RECORDING DEVICES; STOP LISTENING.

Continue to spot-monitor as the circumstances indicate. Use your judgment as to when to spot monitor because many factors enter into your decision: parties to the call or conversation, precise relationship of the parties, the length of relationship, the number of calls or contacts between parties, present status of the investigation, past conduct of the parties, etc.

VIII. **CATEGORIES OF CONVERSATIONS**

Most conversations will fall within one of the following categories:

A. **"PATTERN OF INVOLVEMENT":**

If during the course of the interception, one or more individuals is identified (by name, nickname, voice, etc.) as a co-conspirator or accomplice of our subjects, and there is no applicable privilege involved (Section F), the "spot monitoring" requirement may be relaxed somewhat as to conversations between our subject and those individuals.

B. **CONVERSATIONS INVOLVING UNKNOWNS:**

When a conversation involves one or more unknown individuals, listen and record the conversation for up to two minutes (unless you are satisfied before then that the conversation is not, and is unlikely to become, pertinent). Many courts have agreed that two minutes is a reasonable period for monitoring agents to listen to a conversation before deciding whether it relates to the violations of law under investigation. If after this two minute period it appears that the conversation does not relate to the violations under investigation, TURN OFF THE RECORDER and STOP LISTENING TO THE CONVERSATION.

However, it is possible that at some time after this initial period, one or more of the targets may join the conversation, and/or the conversation may turn from innocent, unrelated topics to the violations under investigation. We have the right to SPOT MONITOR apparently innocent conversations to guard against such a possibility (particularly since we may anticipate that members of the violations under investigation will deliberately try to delay and disguise discussion of those violations to frustrate the use of the interception).

Periodically reactivate the recording and listening devices. Listen to and record the conversation for a brief period. If during this period you hear evidence pertaining to the violations under investigation, continue to listen and record; if not, DEACTIVATE THE LISTENING AND RECORDING DEVICES.



RIF

# Sample of Minimization Memorandum (page 5)

C. **PATTERNS OF INNOCENCE:**

If, after a period of time, we have learned that conversations between particular individuals are invariably innocent, not crime-related, then a "Pattern of Innocence" exists and such conversations should not be recorded, listened to, or even spot-monitored unless exigent circumstances exist.

D. **EXIGENT CIRCUMSTANCES:**

Under special circumstances, it may be necessary to record and listen to conversations which normally would not be intercepted.

If you anticipate such circumstances, consult me at once.

IX. **EVIDENCE OF OTHER CRIMES: ACTION REQUIRED**

We do not have authorization to overhear evidence concerning the commission or planning of other crimes. This interception must be conducted with our sole legal purpose in mind: interception of conversations between our named subjects and co-conspirators and accomplices concerning those federal violations enumerated in the Court Order. Interception of non-enumerated offenses must be brought to my attention immediately.

X. **USE OF LISTENING AND RECORDING DEVICES**

No interception or recording device is to be left unattended on "automatic." "MINIMIZATION" requires that monitoring agents determine whether or not each conversation is relevant and subject to interception.

Anytime a conversation or any part thereof is monitored it is to be recorded. If the interception or recording device has a separate monitor switch, the switch is not to be activated unless you are recording. However, if the interception or recording device malfunctions, or a recording tape has just run out, monitoring is permissible while the situation is being remedied. Be sure to report the overheard conversation and the circumstances of this situation in the Consecutive Call Log.

XI. **DAILY REPORT OR LOG**

Abstracts of summaries of each conversation are to be made at the time of interception and are to be included in the Consecutive Call Logs. If the conversation was not entirely recorded, an appropriate notation should be made indicating the incomplete nature of the conversation (e.g., monitoring discontinued) and why the conversation was not completely recorded (e.g., non pertinent, privileged). Where the exact words used by the participants are important, that portion of the conversation should be included in the Consecutive Call Log. Copies of the logs should be delivered to me on the following day.

The logs are to be a reflection of all activity occurring at the listening post and concerning the intercepted calls or conversations as well as the equipment itself (e.g., replaced reel #2 with #3; malfunction of a recorder, etc.). These logs will ultimately be used by you to explain and to reflect your action taken in intercepting or not intercepting a particular communication. Therefore, it is vitally important to succinctly describe parties to the conversation, the nature of the call, and the action taken (e.g., monitor discontinued, not pertinent or privileged, etc.).

The Consecutive Call Log is of extreme importance both for our reports to the issuing judge and ultimately to the court which will litigate the issue of minimization. If you keep an accurate account of the nature of the conversations, our efforts in preparing for any hearing or trial will be minimized.

The judge of the District Court who issued the court order has the right to require us to make periodic reports to him about the progress of the investigation and the manner in which the warrant is being executed. I will need this information in order to comply with the reporting requirement.

I must receive a copy of all logs, transcripts, and surveillance reports daily!

If anything appears to be breaking suddenly or a problem arises, CALL ME.

Signature

RIF

# Disclosure of Intercepted Communications

Strict guidelines have been established relative to the disclosure and use of communications seized during non-consensual interceptions. 18 U.S.C. 2517 sets forth who may disclose or use information derived through electronic surveillance, and to whom the information may be disclosed, and how the information may be used. Information can be disclosed to, or used by, the following individuals:

(1) To another law enforcement officer for proper performance of his/her official duties;

(2) Any law enforcement officer who legally obtained the information may use the information in proper performance of his/her official duties;

(3) While giving testimony under oath in any proceeding held under the authority of the United States;

(4) Privileged information can not be disclosed (i.e., husband/wife, lawyer/client, doctor/patient, clergyman/parishioner);

(5) The information related to other offenses may be used in accordance with the above sections when a judge of competent jurisdiction approved interception;

(6) To any other Federal law enforcement officer or agency (intelligence, protective, immigration, national defense, national security, etc.) to assist the officials in the performance of his/her official duties;

(7) To any foreign law enforcement officer to the extent that such disclosure is appropriate to the proper performance of his/her official duties and in accordance with the Privacy Act. The foreign law enforcement officer may also disclose or use the information in the performance of his/her official duties;

(8) To any appropriate Federal, State, local or foreign government officials for the purpose of preventing or responding to a threat.

The contents of an intercepted communication is to be disclosed by an agent or attorney only after he/she is satisfied that the person to whom disclosure is made has a need to know the information. Disclosure of intercepted communications to any other investigative agency, pursuant to 18 U.S.C. 2517, should be made only after the Supervising Agent and supervising AUSA have agreed on such disclosure.

A memorandum of disclosure should be prepared by the investigative or law enforcement officer making the disclosure. This memorandum should indicate the name and agency of the person to whom disclosure was made, the date of disclosure, a brief summary of the information disclosed, identification of the interception (call number, etc.) and the purpose for making the disclosure. The investigative or law enforcement officer making the disclosure must inform the recipient that the disclosed information came from an authorized interception, and that subsequent authorization must be obtained before use in any proceeding. Any disclosure of the contents of intercepted communications, by Government attorneys and agents or any other person, which is not pursuant to 18 U.S.C. 2517, may subject the offending party to a civil action for damages under Title 18 U.S.C. 2520.

# Preliminary Meeting Held by Supervising Attorney (AUSA)

In anticipation of the issuance of the court order, but prior to the initiation of the interception, the supervising AUSA should hold a meeting with the Supervising Agent, case agent, all prospective monitoring personnel,

all transcription personnel, all TSD personnel, and headquarters representatives (ISD, et al.) involved with the interception operation. During this meeting, the supervising AUSA should inform all participants of the contents of the anticipated court order, emphasizing those provisions of the court order describing the type of communication sought for interception, the particular violations of law to which the communications relate, the guidelines for minimization, and the guidelines for terminating the interception when the objective has been attained.

The supervising AUSA should emphasize that any limitations in the court order relating to limited hours of operation, visual surveillance, etc., should be strictly followed. All personnel should be briefed on the rules relative to the disclosure of intercepted communications. Prior to participating in any of the specific functions associated with the interception, all personnel involved with the interception must carefully read the following documents:

1. Affidavit supporting the application for the interception order,
2. Application for the interception order,
3. Draft court order submitted for authorization,
4. Minimization memorandum prepared by or for the supervising AUSA,
5. Chapter III of The Interception and Recording of Wire, Oral and Electronic Communication Manual.

After reading these documents, each individual must sign and date the Document Review Log (SSF 3285).

The Document Review Log (SSF 3285) can be found via the USSS Forms Library at Intranet address http://ssweb/mno/pars/forms.

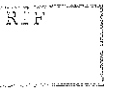
## Posting the Court Order

Since the interception must be confined to the terms of the court order, the order must be posted in the wire room, near monitoring personnel, for quick reference.

## Installation of the Interception Equipment

The only personnel who are authorized to install and test any of the equipment which will be used to accomplish the interception are specialists who are assigned to either the field office or to TSD. Once the equipment has been installed and is operational, these same personnel are responsible for the technical maintenance of the equipment. They should not be utilized for the routine operation of the recording equipment, i.e., maintaining the recorder, monitoring, etc., nor should they become involved in any other non-technical segment of the investigation. All routine operational functions which involve the operation of the intercept equipment should be performed by wire room personnel only.





## Pen Register

Whenever it is anticipated that a non-consensual interception is to be applied for, a request for the installation of a Pen Register should immediately be initiated. The Pen Register is an integral part of most non-consensual interceptions, and its use prior to the interception can provide additional probable cause needed in the application. Early installation of a Pen Register will also facilitate the initiation of the interception once it is authorized by the court. As stated earlier, Pen Register operation is covered under Title III of the Electronic Communications Privacy Act of 1986.

A separate Pen Register should be requested for each target telephone. Prior to requesting the installation of a Pen Register, Chapter IV of this manual should be read in its entirety by all of the investigating and supervisory personnel who will be directly involved in the conduct of the interception.

## Personnel Access

As soon as the Pen Register is installed and operational, the wire room should be considered secure and accessible to only authorized personnel who are directly involved with the interception.

At this time, a "Personnel Access Log" (SSF 3285A) must be posted and maintained at the entrance to the wire room. All persons who access the wire must make the appropriate entries in the log each and every time they either enter or exit.

## Headquarters Notification After Interception Is Initiated (Initiation Message)

As stated earlier, as soon as a judge has issued the interception warrant, 18 U.S.C. 2518(5) requires that the authorization to intercept be executed as soon as practicable. Immediately following the initiation of the interception, the SAIC of the office conducting the interception must submit an official message to headquarters under the case number of the investigation for which the interception is conducted. The distribution of this official message will include the appropriate operational division, the appropriate Assistant Directors Office, the Technical Security Division (TSD), and the Investigative Support Division (ISD). This official message should comment on the following factors:

1. Target telephone (or IP addresses) number(s) and subscriber(s) (area code and number; subscriber name and address),

2. Location of target telephone(s) (or Internet Service Provider) (apartment number, complete address),

3. Court order number, date and judicial district (date signed by judge),

4. Date and time interception initiated,

5. Anticipated duration of use (number of days).

If, during the course of the interception, new target line(s) are identified and approved for interception, an official message(s) must be sent notifying Headquarters of their initiation.

The following page has a sample official message for reporting the initiation of an interception.

# Sample Official Message Reporting the Initiation of a Non-Consensual Interception

FROM: SAIC-FIELD OFFICE

CASE NUMBER:

CASE TITLE:

TO: SAIC-APPROPRIATE OPERATIONAL DIVISION

INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE
SAIC- INVESTIGATIVE SUPPORT DIVISION
SAIC-TECHNICAL SECURITY DIVISION

SUBJECT: INITIATION OF NON-CONSENSUAL INTERCEPTION

REFERENCE IS MADE TO (OFFICE) OFFICIAL MESSAGE DATED _____, REPORTING THE SUBMISSION OF A NON-CONSENSUAL INTERCEPT APPLICATION TO THE DEPARTMENT OF JUSTICE.

INTERCEPTION ORDERS HAVE BEEN GRANTED AND INTERCEPTIONS HAVE BEEN INITIATED FOR THE FOLLOWING TARGET TELEPHONE LINES (OR IP ADDRESSES):

NAME OF THE TARGET:

TARGET TELEPHONE NUMBER (OR IP ADDRESSES) AND SUBSCRIBER: (AREA CODE AND NUMBER; SUBSCRIBER NAME AND ADDRESS)

LOCATION OF TARGET TELEPHONE (OR INTERNET SERVICE PROVIDER): (APARTMENT NUMBER, COMPLETE ADDRESS)

COURT ORDER NUMBER, JUDICIAL DISTRICT AND JUDGE:

DATE AND TIME INTERCEPTION ORDERS GRANTED: (DATE SIGNED BY JUDGE)

DATE AND TIME INTERCEPTION INITIATED/ACTIVATED:

ANTICIPATED DURATION OF USE: (NUMBER OF DAYS)

FIELD OFFICE

CASE SA/SUPERVISOR/SAIC

# Preparation and Logging of Recording of Intercepted Communication

18 U.S.C. 2518(8) (a) directs that the contents of any intercepted communication "...shall, if possible, be recorded on tape... or other comparable device." This requirement is mandatory in all but the most extraordinary situations. Although the mechanical breakdown of recording equipment would probably be temporarily excusable under this section, the preferred practice is to provide for recorder redundancy in an effort to avoid such a situation.

# Recording of Intercepted Communication

Currently, the communication interception equipment employed by this Service utilizes two (2) high capacity recordable disks. The interception equipment can also store the intercepted communication on its hard drives.

The two high capacity disks will be utilized simultaneously for each target telephone line during the wiretap operation. One will be the "Primary Evidence" disk; the second disk will be the "Back-up" disk. The intercepted communication saved on the hard drive may be used to produce the work copy. Only the pertinent communication may be copied on the work copy for transcription.

The high capacity disks will be provided by TSD. Each of the disks will be digitally recorded with case number, case title, disk number, and the phone number intercepted by the wire room personnel. The disk cover will also be labeled with the same information.

All "Primary Evidence" disks may be pre-numbered prior to beginning interception in sequential order for use throughout the entire operation. A suffix letter of "E" (evidence) will follow the assigned disk number (example: Disk # - 001E). The disk numbers must be digitally recorded on the disk. The "Primary Evidence" disk should be replaced when the maximum capacity of disk space is filled. It is the responsibility of the Shift Leader to record the call number sequence (example: disk number - 001E, Call numbers - 001 to 100) on the disk label. The disk will be then placed in a Title I Evidence Control Record (SSF 3277) envelope. The wire room Shift Leader will make the appropriate entries on the envelope. Form SSF 3277 can be obtained from ISD.

A second disk will be utilized to record a "back-up" of the evidence disk. The "back-up" disk should also be pre-numbered in sequential order for use throughout the entire operation. The number of each disk will coincide with the "Primary Evidence" disk number, except that the suffix letter of "B" (back-up) will follow the number (example: 001B). The disk numbers must be recorded on the disk and disk label. The back-up (B) disk will be replaced at the same time as the evidence (E) disk. The disks will then be placed in a separate SSF 3277 (Title I Evidence Control Record) and the wire room Shift Leader will make the appropriate entries on the envelope. Form SSF 3277 can be obtained from ISD.

Only the pertinent conversations may be recorded using the data saved on the hard drive of the computer used in the interception. These separate recordings may be used to transcribe by the transcribing personnel. Each "work" disk containing pertinent conversations will be secured in a Title I Evidence Control Record (SSF 3277) after the conversation has been transcribed.

The SSF 3277's containing evidence, backup, work copy, transcript, and consecutive call log will be inventoried on SSF 1544 per the procedures outlined in INV-15.

## Procedure When No Recording Can Be Made

As was stated earlier, absent exigent circumstances, the contents of any intercepted communication shall be recorded on a tape or technologically comparable storage device. In those unusual situations where an interception cannot be recorded, (e.g., equipment failure) the intercepting agent must submit a memorandum reporting the contents of the interception.

This memorandum should be as near a verbatim transcript as possible under the circumstances of the interception, and should outline the circumstances that prevented the recording of the interception. The memorandum should indicate the date, time, and place of the interception, the court order authorizing the interception, and should be signed by the intercepting monitor. Upon completion, the memorandum should be treated as though it was a recording of the conversation, and secured in a Title I Evidence Control Record, SSF 3277, and the wire room Shift Leader will make the appropriate entries on the envelope.

## Disk Control Log

The Disk Control Log (SSF 3279A) is a record of the installation and removal of the "Primary Evidence" and "Back-up" disks and will be maintained by the Shift Leaders in the wire room. The "Work" disks are not entered into this log. All installation and removal of "Evidence" or "Back-up" disk will be recorded in the Disk Control Log.

The Disk Control Log (SSF 3279A) can be found via the USSS Forms Library at Intranet address http://ssweb/mno/pars/forms.

## Consecutive Call Log

The interception equipment currently employed by this Service generates the Consecutive Call Logs automatically and allows the operator to input all information pertaining to the call directly into the interception equipment during the interception of communication. The monitoring personnel shall input the necessary information into the equipment contemporaneous to intercepted phone communication in order to maintain accurate records. Some of the required information includes, whether the call is pertinent or non pertinent, synopsis of the call, and whether the call was or was not minimized. The call information, to include dialed number, duration of call, and incoming or outgoing call status, will be provided by the interception equipment automatically.

The Consecutive Call Log generated by the interception equipment will be printed daily at a predetermined time and will be handled as evidence. Three copies of the Consecutive Call Log will be made. The original will be secured in a Title I Evidence Control Record envelope (SSF 3277). One copy each will be provided to the case agent and AUSA. The remaining copy will be retained by the wire room Shift Leaders for use of wire room personnel.

If the monitoring personnel are unable to maintain the Consecutive Call Log via the interception equipment, the Title I Consecutive Call Log (SSF 3279) will be used to record necessary information.

The Title I Consecutive Call Log (SSF 3279) can be found via the USSS Forms Library at Intranet address http://ssweb/mno/pars/forms.

# Interception of Electronic Communication

The procedures for obtaining authorization remains the same as previously prescribed. Processing of evidence differs slightly as compared to interception of oral communication.

Processing evidence from electronic communication interceptions involves "After the Fact Minimization." A thorough review of the "evidence handling" procedures should be discussed with the AUSA.

In addition, interception of electronic communication requires slightly different configuration than the traditional Title I interception. Interception of electronic communication requires a minimization team, investigative team, and technical support team.

Intercepted communication will be downloaded by the minimization personnel at the predetermined time each day by transferring the e-mail/fax/chat/other files from the server's mainframe to the hard drive of the minimization personnel's computer terminal. Each transfer of data will be logged on the Activity Log and maintained by the minimization team. The minimization personnel will take necessary precautions to ensure the integrity of intercepted data during transfer from the server's mainframe and while reviewing and sorting into appropriate categories.

The minimization team will review all intercepted communications and a determination should be made whether they are pertinent or non pertinent; considering the identities of the sender, the recipient, the content of the transmission and other available information. The data should then be indexed into three categories. These categories are "Pertinent," "Non Pertinent," and "Unknown."

On the computer used to download and review the data, the minimization team will create three folders. These folders are "Pertinent," "Non Pertinent," and "Unknown." Each of the folders will also contain three sub folders. These subfolders are, "Chat," "E-mail/fax," and "Other."

All chat/instant messaging deemed pertinent will be reviewed and moved to the "Chat" folder of the "Pertinent" folder. All e-mails and faxes deemed pertinent will be reviewed and moved to the "Email/fax" folder of the "Pertinent" folder. All others, i.e. downloads and web browsing deemed pertinent, will be reviewed and moved to "Other" folder of the "Pertinent" folder.

All chat/instant messaging deemed non pertinent will be reviewed and moved to "Chat" folder of the "Non Pertinent" folder. All e-mails and faxes deemed non pertinent will be reviewed and moved to the "Email/fax" folder of the "Non Pertinent" folder. All others, i.e. downloads and web browsing deemed non pertinent, will be reviewed and moved to the "Other" folder of the "Non Pertinent" folder.

If the minimization team is unable to make a determination as to pertinent or non pertinent, the intercepted data should be moved to the "Unknown" folder. Every effort should be made to make the determination whether they are pertinent or non pertinent. The minimization team may consult with the investigative team without disclosing whole communication to determine whether the communication is pertinent or not.

Evidence of other crimes should be moved to the "Other" subfolder in the "Unknown" folder until the AUSA supervising the interception is notified and the court order is amended to monitor other crimes not authorized in the original court order.

Any data containing codes, foreign language, or encryption may be placed in the "Unknown" folder until determination is made to whether they are pertinent or non pertinent.

At the end of the interception, the entire intercepted communication/data will be stored on a technologically appropriate storage device. This includes pertinent, non-pertinent, and unknown communications. Also, all pertinent communication will be stored on a separate technologically appropriate storage device.

The storage device containing all intercepted communication/data will be logged, per INV-14 and INV-15, as evidence and sealed at the completion of the interception. The storage device containing only the pertinent communication will also be logged as evidence and properly stored.

A print out of the folder directory should be made and stored along with the storage device. The evidence handling procedures should be discussed in detail with the AUSA supervising the interception.

The investigative team may consist of Agents who are familiar with the case. These agents will have access to only the "Pertinent" folder of the intercepted communication. The investigative team will have minimum contact with the minimization team to prevent undue influence.

The technical support team may consist of TSD or ECSAP trained personnel. If required, outside venders may be utilized in technical aspects of the interception under the supervision of the TSD or ECSAP Agents. The technical support team will ensure all the equipment used in the interception is in proper working condition. They may install, maintain, and test the equipment to ensure working condition. Prior to installation, the technical support team will ensure that all the computers and storage devices are free of contamination.

If an intercepted communication contains privileged information, the AUSA supervising the interception should be notified immediately.

## Transcripts

Generally speaking, it is not necessary to routinely transcribe all of the pertinent conversations that are intercepted. However, if the intercepted conversation is only marginally audible or intelligible, a transcript will probably facilitate the understanding of the conversation. In these cases, it is highly recommended that a transcript be made.

If it is probable that the intercepted conversation will be used during any judicial proceeding, the conversation should be transcribed. Transcripts facilitate the writing of investigative reports, aid in the preparation for judicial proceedings, facilitate the direct and cross-examination of witnesses, enable an attorney to quote relevant portions of conversations during summation, and facilitate appellate review of the trial record.

If the transcripts are to be distributed to the jury, **every effort should be made to ensure that they are as complete and accurate as possible.** If the key evidence in a case consists of recordings which are difficult to comprehend without the use of transcripts, the verdict may depend upon whether the jurors can follow the transcripts and whether the jurors accept them as accurate. An omitted word or phrase, though irrelevant to the importance of the conversation, may reduce the credibility of the transcription of a less easily understood but more important passage. The transcript should also contain auditory signposts to assist the jurors in following the conversation. Inaudible passages should be marked as such, with an indication of how long the inaudible passage is.

Noticeable changes in the volume or character of background noise should be highlighted. Such signposts may enable a juror who has lost his/her place on the transcript to find it again. A transcript which was perfectly adequate for investigative purposes may not be sufficient for judicial presentation.

Transcripts which are prepared during the interception will probably require extensive revision when preparing for trial. The transcription style should be consistent from conversation to conversation. The following information obtained from the computer generated Consecutive Call Log and the disks must be contained in the heading and body of the transcript.

1. Target Telephone Number,
2. Call Number,
3. Date of Call,
4. Page Number (page ___ of ___),
5. Transcriber Name,
6. Date(s) of Transcription (Date In/Date Out),
7. Case Number,
8. Ingoing/Outgoing,
9. "In" Parties,
10. "Out" Parties.

In the case of interception of electronic communication, transcription may not be necessary unless the communication is in codes or in foreign language.

The transcription should be devoid of any editorial insertions. For example, if one of the parties to the conversation referred to "Big Jim," the identity of "Big Jim" should not be inserted in the transcript.

Transcription may be done by non-agent administrative personnel. However, they must work in conjunction with an agent working on the interception; that agent must then review the transcription for accuracy. Copies of all transcripts should be made for both the supervising AUSA and Wire Room Supervisor.

The original transcript is evidence and should be handled as such. Upon completion, the transcript will be placed in a Title I Evidence Control Record (SSF 3277) and secured.

## Termination of the Interception

18 U.S.C. 2518(5) commands that the court ordered interception terminate either when the objective of the surveillance has been realized or on a specified date within 30 days after the start of the interception, whichever comes first. The interceptions of conversations must terminate as soon as the Government has obtained the evidence which was the objective of the authorization. If the interception is continued beyond that point, evidence derived from continued interception will not be construed as obtained pursuant to a court order.

Such an unauthorized interception would violate the Fourth Amendment and would have three serious consequences: First, evidence derived from the unauthorized interception would be rendered inadmissible. Second, the personnel conducting the unauthorized interception might be subject to criminal penalties. Third, the personnel conducting the unauthorized interception might be subject to civil suit by persons whose conversations were intercepted.

It should be noted that, while many court orders cite the identification of co-conspirators as one of the primary objectives, a blind reliance upon this language as grounds for continuing the surveillance until the calendar expiration date could be subject to serious consequences. While it is true that identifying and defining the

roles of conspirators is a proper objective, it must be realized that these interceptions rarely result in the identification of all participants. The primary consideration is whether a continued interception can stand the test of subsequent court scrutiny.

The Wire Room Supervisor bears initial responsibility for determining when the interception should be terminated. When, during the course of the interception, the Wire Room Supervisor determines that the communications expected to be overheard have been intercepted and recorded, he/she shall immediately consult with the supervising AUSA regarding the decision. If the supervising AUSA does not concur, then interception under the original court order shall continue. If the supervising AUSA determines that sufficient evidence has been obtained from the authorized interception, the electronic surveillance must cease.

Regardless of whether or not an authorized interception has achieved its objective, it may only take place during the period authorized by the court order. When nearing the end of this time period, it is the responsibility of the Wire Room Supervisor to notify the supervising AUSA of the impending termination of the interception. The Wire Room Supervisor must then ensure that the interception is terminated by the time the court order elapses.

## Application for Extension of Interception

In many instances, a court ordered interception will reveal some, but not all, of the evidence sought in the application. On other occasions, the interception will reveal so much evidence that the scope of the investigation must be expanded considerably. In either situation, it may be desirable to continue the interception of the target telephone or apply for authorization for the interception of additional target telephones. The AUSA, in consultation with the Wire Room Supervisor and Case Agent, will make the decision as to whether or not an application for extension is appropriate.

18 U.S.C. 2518(5) provides as follows:

> **"...No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days..."**

Any application for the extension of a court ordered interception must satisfy all of the statutory provisions which govern the initial application and court order. Although Title I does not place a limit on the number of extensions that may be applied for, the courts look very carefully at extended use of court ordered interceptions.

Applications for extensions by the AUSA can often be processed in three or four days, but the time frame can vary widely. If it is important that the electronic surveillance not be interrupted, the extension request must be submitted to the AUSA with sufficient lead time.

When a time gap exists between the termination of the original interception and the signing of the extension order, it is not necessary that the interception facilities be removed or dismantled. It is sufficient that they be

deactivated, that is, turned off. **During this period it is imperative that interception personnel understand that they do not have authority to intercept or record communications unless and until the court signs the extension, and even then their authority is circumscribed by the terms of the extension order and not the original.**

During the extension interception, the same procedures should be followed as during the original interception. Headquarters must be notified via official message upon the initiation of the extension.

## Final Headquarters Notification (Termination Message)

Immediately following the termination of each interception, the SAIC of the office conducting the interception must submit an official message to headquarters under the case number of the investigation for which the interception was conducted. The distribution of this official message will include the appropriate operational division, the appropriate Assistant Directors Office, the Technical Security Division (TSD), and Investigative Support Division (ISD).

This official message will reference the previous Headquarters initiation official message reporting initiation of the interception.

This official message will certify the termination of use, disconnection and removal of all of the interception equipment and should comment on the following factors:

1. Target telephone number (or IP addresses) and subscriber (area code and number; subscriber name and address);

2. Location of target telephone (or Internet Service Provider) (apartment number, complete address);

3. Court order number, date and judicial district (date signed by judge);

4. Date and time of interception termination;

5. Duration of use (date and time it was first operational through date and time it was disconnected; total number of days operational);

6. Investigative benefits derived (brief synopsis);

7. Security specialist completing the removal of equipment;

8. Telephone company representative notified of removal (title, name and telephone number);

9. Location equipment removed from (location name and address).

# Sample Headquarters Notification Official Message for Reporting the Termination of a Non-Consensual Interception

FROM: SAIC-FIELD OFFICE

CASE NUMBER:

CASE TITLE:

TO: SAIC-APPROPRIATE OPERATIONAL DIVISION

INFO: AD-APPROPRIATE ASSISTANT DIRECTORS OFFICE
SAIC-TECHNICAL SECURITY DIVISION
SAIC-INVESTIGATIVE SUPPORT DIVISION

SUBJECT: TERMINATION OF NON-CONSENSUAL INTERCEPTION

REFERENCE IS MADE TO OFFICIAL MESSAGE, DATED _____, REPORTING THE INITIATION OF THIS NON-CONSENSUAL INTERCEPTION. THIS INTERCEPTION HAS BEEN TERMINATED.

NAME OF THE TARGET:

TARGET TELEPHONE NUMBER (OR IP ADDRESSES) AND SUBSCRIBER: (AREA CODE AND NUMBER; SUBSCRIBER NAME AND ADDRESS)

LOCATION OF TARGET TELEPHONE (OR INTERNET SERVICE PROVIDER): (APARTMENT NUMBER, COMPLETE ADDRESS)

COURT ORDER NUMBER, DATE AND JUDICIAL DISTRICT: (DATE SIGNED BY JUDGE)

DATE AND TIME INTERCEPTION TERMINATED:

DURATION OF USE: (DATE AND TIME IT WAS FIRST OPERATIONAL THROUGH DATE AND TIME IT WAS DISCONNECTED; TOTAL NUMBER OF DAYS OPERATIONAL)

INVESTIGATIVE BENEFITS DERIVED: (BRIEF SYNOPSIS)

SECURITY SPECIALIST COMPLETING THE REMOVAL OF EQUIPMENT:

TELEPHONE COMPANY REPRESENTATIVE NOTIFIED OF REMOVAL: (TITLE, NAME AND TELEPHONE NUMBER)

LOCATION EQUIPMENT REMOVED FROM: (LOCATION NAME AND ADDRESS)

FIELD OFFICE CASE SA /SUPERVISOR/SAIC)

## Sealing and Custody of the Evidence Upon Termination of Interception

Immediately upon termination of the interception, the original recordings of the conversations (evidence disks, storage devices), the intercepted electronic communication should be submitted by the supervising AUSA to the judge authorizing the interception. The judge will then order these evidentiary items sealed and order their place of custody.

As most courts and their clerks are not equipped to safeguard evidence, the supervising AUSA will probably suggest that the court order the custody of the sealed evidence to remain with the investigating office which undertook the surveillance. In many instances, the bulk of the evidentiary material will preclude their being kept by the clerk of the court.

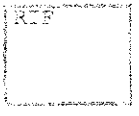
The sealing should be done under the supervision of the authorizing judge. Careful attention should be observed when safeguarding the evidence. If recordings are to be sealed, careful attention must be paid to environmental conditions such as extreme heat or cold or strong magnetic forces which can adversely affect the original condition of the storage devices. Any such conditions must be avoided.

## Inventory - Disclosure of the Wire Tap

Whenever law enforcement officers conduct a search pursuant to the issuance of a warrant, they must subsequently notify the person or persons whose property has been searched and give that person or persons an inventory of the items that have been seized. A similar notice and inventory must be served upon the subject of an eavesdropping warrant. 18 U.S.C. 2518(8) (d) states in part as follows:

> **"Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of -**
>
> **(1) the fact of the entry of the order or the application;**
>
> **(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application and;**
>
> **(3) the fact that during the period wire, oral, or electronic communications were or were not intercepted.**
>
> **The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice..."**





## Postponing of the Inventory - Disclosure of the Wiretap

Congress recognized that the continuing investigation of a subject could be compromised if the inventory invariably was served within the prescribed 90 day period. Therefore, the filing of the inventory may be postponed during a period when the supervising AUSA can demonstrate that there is "good cause" for the postponement. 18 U.S.C. 2518 (8) (d) states in part as follows:

> **"...On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed."**

Whenever the supervising AUSA has reason to believe that there is "good cause" to postpone the serving of the inventory, he/she should immediately file an ex parte motion stating the good cause and requesting postponement. The motion may be made to any judge of competent jurisdiction. Normally, it would be made before the judge to whom application for the order was originally made.

## Preparing the Inventory List for Disclosure of the Wiretap

The Supreme Court has held that 18 U.S.C. 2518 (8) (d) requires the Government, when the intercept is over, to classify all persons whose conversations have been overheard and to provide that information to the issuing judge so that he/she may use it in causing mandatory notice to be served on persons named in the application or order and in exercising his/her discretionary power to have notice served on unnamed persons who were intercepted.

The following are essential classifications:

1. Persons named in the order or the application,
2. Other persons whose intercepted communications apparently incriminate them in the offense or offenses specified in the interception order,
3. Other persons whose intercepted communications apparently incriminate them in offenses not specified in the interception order, and
4. Persons whose intercepted communications are apparently non-incriminating.

If any omission is discovered after the judge has been provided with the classifications, a supplementary report correcting the omission should be made to him/her as soon as possible. To facilitate the preparation of the inventory listing, the supervising AUSA should require the Wire Room Supervisor to furnish him/her a preliminary report detailing the names of those intercepted and the category into which each falls, approximately 90 days after termination of the interception.

The inventory listing should be forwarded by the supervising AUSA to the court approximately 5 days prior to the date that the inventory is due. Attached to the inventory should be a proposed order of those who must be inventoried. The supervising AUSA should assist the judge in the exercise of this function by making recommendations.

Ordinarily, those in the first three of the above categories are inventoried, and those in the fourth category are not. **It is important to insure that every indictee and prospective indictee who has been identified subsequent to the inventory proceedings, is served with an inventory as soon as practicable.**

## Record Retention

As per 18 U.S.C. 2518(8)(a), recordings of intercepted conversations or other evidentiary material (e-mail, faxes, etc.) must be retained, maintained and protected for a minimum of ten years at a location so ordered by the court. The seal placed upon the recordings by the court will not be broken during this maintenance period unless authorized by the court. Upon expiration of the retention period, the recordings may only be destroyed pursuant to court order by the original authority granting interception.

The Secret Service case file and all administrative records pertaining to the investigation shall be retained for a minimum of ten years in the field office (refer to ADM Manual, Section MNO-07(06)). Each case file must have a SSF 3103, Non-Consensual Interception, affixed to the front of the file folder to preclude unauthorized disclosures and to prevent premature destruction of the file. The SSF 3103 may be obtained from ISD.

**A copy of the inventory submitted to the supervising AUSA, and a list of all telephone numbers associated with subjects on this inventory list, is forwarded to ISD for inclusion in the electronic interception file. Other documents included in the electronic interception file are all court orders, affidavits, applications, extensions, and minimization instructions.**

## Indexing of the Targets in MCI

It is the responsibility of the controlling field office to ensure that all pertinent information is entered into the MCI system. During the indexing of subjects intercepted under the court order, subject interest codes 42 and 43 will be used in conjunction with other codes (suspect or defendant). Interest code 42 will be used to identify subjects who are being intercepted or who have been intercepted by this Service. The subjects will include primary targets of an investigation, as well as any additional targets who may become a suspect or a defendant. Interest code 43 will be used to identify subjects who are being intercepted or who have been intercepted by other law enforcement agencies.

The interest codes 42 and 43 may be entered by the field office personnel. However, modification of the codes can only be done by ISD personnel. The new interest codes will not affect the status or closing of the case.

In addition to updating the subject screen with the interest codes 42 and 43, the Subject Summary (SSUM) will also be updated with the subject's telephone numbers, address, date of interception, agency conducting the interception and other pertinent information to include charges, sentencing information, and whether the subject is a primary target of the investigation or was an additionally developed target. In the case of intercepted faxes, this will include all subjects, fax numbers and addresses. In the case of intercepted email, this will include email addresses and internet protocol addresses.

## Reports to Department of Justice

Title 18 U. S. C. 2519 requires that in January of each year this Service provide to the Attorney General of the United States an annual report of all interceptions conducted in the prior twelve (12) months. This report will cover each application for any non-consensual wire, oral, and electronic interception made by this Service under provisions of the Omnibus Crime Control and Safe Streets Act of 1968 and the Electronic Communications Privacy Act of 1986.

This annual report will be compiled by the Investigative Support Division (ISD) with input from the field and will be reported on Court Forms WT1 (Annual Prosecutor Summary of Wiretap Reports), WT2 (Report of Application and/or Order Authorizing Interception of Communication), and WT3 (Supplementary Report for Wiretaps Reported in Previous Calendar Years). Office of Enforcement Operation (OEO), DOJ will provide instructions on completion of the required forms.

The completed forms (WT1, WT2, and WT 3) will be forwarded, under covering memorandum from the Office of the Director to Office of Enforcement Operations (OEO), DOJ.