Consensual Interceptions
Table of Contents

Page

United States Secret Service
Directives System

Manual : Interception
RO : ISD

Section : Chapter II
Date : 08/06/2009

Subject: Consensual Interceptions

To: All Supervisors and All Manual Holders of the Interception and Recording of Wire, Oral, and Electronic Communications Manual

Filing Instructions:

- Remove and destroy the Chapter II Table of Contents (dated 03/01/2006), and replace with the attached revised Table of Contents.
- Remove and destroy Chapter II, Consensual Interceptions (dated 03/01/2006), in its entirety and replace with the attached revised chapter.
- File this Policy Memorandum in front of this section.
- This directive is in effect until superseded.

Impact Statement: This directive has been updated to remove language that could compromise ongoing investigations of additional subjects or criminal websites. More specifically, language has been removed from pages 15 and 16 that allowed "working copies" to be made of computer hard drives as they are not needed for continuing investigations.

Mandatory Review: The Responsible Office will review all policy contained in this section in its entirety by or before August 2012.

Questions regarding this policy should be directed to the Investigative Support Division at 202-406-5773.

D S. John

POR Michael Merritt
AD - Investigations

DCP#: WIM 2009-02

RIF

CONSENSUAL INTERCEPTIONS

Introduction

Pursuant to the provisions of Title 1, it is not necessary to obtain a court order in situations where one or more parties to a communication have given their prior consent to the interception or recording of their conversations. Title 18 U.S.C. 2511 (2)(c) states that "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."

The monitoring of conversations with the consent of one of the participants is a particularly effective and reliable investigative technique; and its use by the U.S. Secret Service (USSS) during a criminal investigation is encouraged where appropriate, and is expected where necessary. Nevertheless, although it is clear that such monitoring is constitutionally and statutorily permissible, it is appropriate that this investigative technique continue to be closely regulated.

For this reason, specific administrative guidelines and procedures have been established by the Department of Justice (DOJ) and the U.S Secret Service. These guidelines and procedures address two categories of consensual interceptions; non telephonic to include electronic communications, and telephonic.

Secret Service Policy

Reference is made to the Attorney General's memorandum dated May 30, 2002, entitled "Procedures for Lawful, Warrantless Monitoring of Verbal Communication." This memorandum allows the Director to delegate this authority to other supervisors within the USSS. Accordingly, the Director has issued a delegation of authority for the authorization of these interceptions. This delegation of authority is reproduced as follows:

DELEGATION OF AUTHORITY

NO. 34 REVISION NO. 4

INTERCEPTION OR RECORDING OF CONVERSATIONS WITH THE CONSENT OF ONE PARTY BY SECRET SERVICE PERSONNEL

In accordance with the Department of Justice U.S. Attorneys' Manual, 9-7.301, Consensual Monitoring, the following officials of the U.S. Secret Service are hereby delegated the authority to approve and to implement the monitoring of private conversations with the consent of one party, in limited contexts as set forth in, and pursuant to, the guidelines promulgated by the Attorney General dated May 30, 2002:

Non-telephonic and Telephonic Interceptions

Assistant Director – Office of Investigations
Assistant Director – Office of Protective Research
Assistant Director – Office of Professional Responsibility
Deputy Assistant Director(s) – Office of Investigations
Deputy Assistant Director(s) – Office of Protective Research
Deputy Assistant Director(s) – Office of Professional Responsibility
Special Agent in Charge – Office of Protective Intelligence and Assessment Division
Special Agent in Charge – Office of Criminal Investigative Division
Special Agent in Charge – Office of Investigative Support Division
Special Agents in Charge – USSS Field Offices

This authority may be delegated to the Deputy Special Agent in Charge (DSAICs), Assistant Special Agent in Charge (ASAICs), and Resident Agent (RAICs) acting in the capacity of the Special Agent in Charge(SAICs) enumerated above.

This delegation supersedes USSS Delegations of Authority No. 34, Revision No. 3, dated November 6, 2000.

Consensual Interceptions and/or Recordings of Telephonic and Non-Telephonic Communications

Department of Justice Policy

Department of Justice (DOJ) administrative guidelines and procedures governing the use of consensual non-telephonic interceptions are outlined specifically in the Attorney General's memorandum dated May 30, 2002, entitled "Procedures for Lawful, Warrantless Monitoring of Verbal Communication." This memorandum, hereinafter referred to as "the Attorney General's memorandum," is the basis for all USSS guidelines and procedures set forth in this chapter.

Specific authorization and reporting procedures have been established for use during **all** consensual interceptions of telephonic and non-telephonic communications. In most cases, these authorization procedures do not require prior written authorization from the DOJ, Office of Enforcement Operations (OEO). However, in a number of "sensitive" cases, prior written approval for the interception must be granted by the Director or Associate Director of the OEO, DOJ.

Cases Requiring Prior Written Department of Justice Approval

In all but the most sensitive cases, the authority to approve requests for consensual surveillance is transferred to the departments and agencies.

There are six sensitive types of cases that require formal written approval from the DOJ. These sensitive cases require approval in writing by the Director or Associate Director of the Office of Enforcement Operation (OEO), Criminal Division, U.S. Department of Justice. These cases will be coordinated through the Investigative Support Division (ISD)

Prior to submitting a request for approval to the OEO, the investigator must first discuss with the Assistant United States Attorney (AUSA) the appropriateness and legality of the consensual monitoring. Upon concurrence from the AUSA, the investigator will make a formal request to the DOJ (OEO) with the approval of the Director or his designee. (See the Delegation of Authority on page 1 of this chapter.)

An emergency request may be made by telephone to the authorizing official and should later be memoralized in writing and submitted to the appropriate headquarters official as soon as practical after authorization has been obtained

If an emergency situation requires consensual monitoring and the approving official can not be reached, the authorization may be given by the Director or his/her authorized designee (Per Delegation of Authority). No later than three working days after the emergency authorization, this Service must notify, in writing, OEO, of the emergency monitoring.

The six "sensitive" case categories are as follows:

1. **High Federal Officials.** Investigations involving such sensitive investigative tools such as those utilized in consensual monitoring must be approached with extra care when the non-consenting party is a high Federal official. The officials delineated are: Members of Congress, Federal Judges, and any other Federal official holding a position of Executive Level IV or above, or a person who has served in this capacity within the last two years. This group includes Cabinet members, members of the White House staff, and most Presidential appointees. Investigations involving such officials must be supervised and coordinated at a central point, particularly since such investigations may raise issues involving the application of the Special Prosecutor provisions of the Ethics in Government Act of 1978. This category encompasses all of the major positions covered by that Act.

2. **Other Public Officials.** The Department of Justice has deemed it inappropriate to require central authorization in all cases in which other public servants, both Federal and State, are non-consenting parties because of the size and scope of the Federal and State work force and the wide variety of offenses that might be involved. However, certain offenses involving Federal or State public officials strike at the very integrity of Government. Thus, in cases in which a public official is the target of the investigation and the alleged offense involves **bribery, conflict of interest,** or **extortion** relating to the performance of official duties, centralized Department of Justice control will be retained.

3. **Members of the Diplomatic Corps.** Consensual surveillance of members of the diplomatic corps of a foreign country raises questions concerning the foreign relations of this country. To ensure appropriate coordination with the U.S Department of State in this sensitive area, formal written approval from the Department of Justice is required is required before consensual monitoring is utilized.

4. **Protected Witnesses.** It is vital to the integrity of the Witness Security Program that controls be maintained regarding the manner in which witnesses in the program, or those known to have been in the program, are properly utilized. For instance, use of a protected witness as an undercover informant can expose him/her to extreme danger, greater than that faced by other undercover informants. Centralized control is important in this area as well.

5. **Federal Prisoners.** The use of a monitoring device involving a person in the custody of either the Federal Bureau of Prisons or the United States Marshals Service raises particularly sensitive issues not the least of which concerns the Fifth Amendment right to counsel. It is also vital to prisoner security and safety that the Bureau of Prisons and the Marshals Service be informed whenever possible of consensual monitoring activities in their institutions or involving their charges; this is true whether the consenting person is or is not the prisoner. Authorization in such cases must be centralized in the Department of Justice. (Procedures on the use of Federal Prisoners are outlined in Investigative Manual, section ISD-08.)

6. **Where Otherwise Requested by the Department of Justice.** The final category consists of specific cases in which a written request from a United States Attorney or a higher Department of Justice official is deemed necessary for the proper progress of an investigation. This determination will be made by the United States Attorney(s) or officials of higher position within the Department of Justice.

Exceptions

Even if the interception falls within any of the six aforementioned categories, prior Department of Justice approval **is not** required for:

1. Extraterritorial interceptions;

2. Foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, **et seq.**);

3. Interceptions pursuant to the court-authorization procedures of Title I & III of the Omnibus Crime Control and Safe Streets Act of 1986 as amended (18 U.S.C. 2510, **et seq.**);

4. Routine Bureau of Prisons interceptions of verbal communications which are not attended by a justifiable expectation of privacy;

5. Interceptions of radio communications; and

6. Interceptions of telephonic communications.

Cases Not Requiring Prior Department of Justice Approval

If an interception which is to be made does not fall within the six "sensitive" case situations, no prior written Department of Justice authorization is required.

Authorization Procedures for All Consensual Telephonic and Non-Telephonic Interceptions

All interceptions must be authorized by the head of the department or agency or his/her authorized designee (See Delegation of Authority), on page 1 of this chapter). However, prior to receiving approval, a representative of the department or agency (usually, the case agent) must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation.

The requirement for approval is based on the Attorney General's memorandum titled "Procedures for Lawful, Warrantless Monitoring of Verbal Communications" dated May 30, 2002, which allows approval for the interception by the Director or his/her designee.

Whenever possible, authority to conduct an interception should be requested at least 48 hours prior to the interception.

If the interception falls within any of the six "sensitive" case situations requiring prior Department of Justice approval, the request for approval shall be made to the Department of Justice by the appropriate operational division, through the Investigative Support Division (ISD).

Additionally, the following guidelines, promulgated by the U.S. Department of Justice, will apply to inmate telephone conversations monitored by the Federal Bureau of Prisons:

1. Prison officials can monitor inmate telephone conversations for the purposes of maintaining prison security and prison administration. Attorney/client calls, however, are obviously excluded.

2. Law enforcement authorities outside of the Bureau of Prisons are not allowed random access to inmate monitored telephone conversations, past, present or future.

3. Requests by outside law enforcement agencies to disclose transcripts of the general telephone conversations of inmates that have been monitored in the past, in connection with a criminal investigation relating to activities outside the confines of the prison and concerning specified individuals, will be complied with only pursuant to a proper legal authorization, (e.g., grand jury subpoena, search warrant, or subpoena issued by the court).

4. Requests by outside law enforcement agencies to monitor and disclose the future telephone conversations of specified inmates in connection with a criminal investigation being conducted, relating to activities outside the confines of the prison that do not affect prison security or administration, will be complied with only where an interception order has been procured under the authority of Federal statutes pertaining to electronic surveillance, 18 U.S.C. 2510 **et seq.**

In addition, it should be noted that inmate/attorney telephone monitoring requires a court order, absent a clear showing that there is no attorney client privilege involved. Also, in cases of consensual telephone monitoring involving prisoner use requests (see Investigative Manual, section ISD-08), permission for telephone monitoring may be appended upon request, in the initial communication requesting the use of the prisoner.

28 C.F.R. 540.102, directs the warden of a Federal correctional institution to give notice to the prisoners of the potential for monitoring their conversations.

Examples of Consensual Non-Telephonic Interceptions and/or Recordings

1. The use of a transmitter or recorder secreted on the person of an agent or informant while engaged in conversations with a suspect or suspects.

2. The installation of a transmitter or recorder in a fixed location, without trespass, where an agent or informant is engaged in conversation with a suspect or suspects. (Unless an agent or person is acting pursuant to court order that authorizes entry and/or trespass.)

   (**NOTE:** Should the consenting party leave the location where the transmitter or recorder is installed, the interception and/or recording of further conversation between the non-consenting parties must terminate immediately. Continued interception would require a court order under Title I.)

3. Electronic Communication intercepted over a modem or network connection. Additional information is available on page 14 of this policy under the section entitled "Electronic Communications Consensual Intercepts."

Examples of Consensual Telephonic Interceptions and/or Recordings

1. Phone call to or from a consenting person, agent or otherwise, to a suspect while a second agent listens on an extension telephone.

2. Phone call to or from a consenting person, agent or otherwise, to a suspect while a second agent overhears the conversation on speaker-type phone equipment.

3. Phone call to or from a consenting person, agent or otherwise, to a suspect while a stenographer records the conversation in shorthand while overhearing the conversation.

4. Phone call to or from a consenting person, agent or otherwise, to a suspect which is recorded. This example is considered to be included within the above guidelines even though the conversation is not listened to by a third party until the conversation has been concluded, i.e., by playing the recording. As in non-telephonic intercepts, tape cassettes or disks used in recording consensual telephonic intercepts should be properly labeled. All evidence should be handled in accordance with evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Resources Section of the Forensic Services Division (FSD) Homepage.

Reporting of Consensual Non-Telephonic Interceptions

Within two (2) days following any interception, an official message must be forwarded to the appropriate operational division, appropriate Assistant Director's Office, and the Investigative Support Division (ISD). This official message should be submitted under the case number of the investigation in which the interception has been conducted. If a local field office case number has been assigned, it **must** be designated Special ("S"). This official message will be part of the case file maintained at the field office and at the appropriate operational division. (See the section entitled "Electronic Communications Consensual Intercepts" on page 14 of this policy for electronic communication intercept reporting requirements.)

This official message shall comment on the following factors:

- Name of the United States Attorney, Assistant United States Attorney or Organized Crime Strike Force attorney who provided advice as to the legality of the consensual interception, date of advice, and the judicial district to which he/she is assigned;
- Reason for the interception;
- Whether or not the target of the interception falls within any of the six "sensitive" case situations. If yes, explain (see the six "sensitive" case categories listed in this chapter);
- Type of equipment used;
- Equipment serial and/or USSS property number;
- Whether or not a recording was made (if no, state reason why, i.e., equipment failure, etc.);
- Method of installation;
- Location where equipment was used (include judicial district);
- Name(s) of all person(s) intercepted, include all aliases, dates of birth, and Social Security numbers if available, or "unknown subject." (The name(s) of the person intercepted for which permission to intercept as a target was obtained should be listed first, and should be denoted as a target);
- Name of consenting party;
- Date of interception;
- Duration of interception;
- Investigative benefits derived (Be specific if no benefits were derived); and
- Is continued use expected? Yes or No.

When any authorization is granted, it applies to only those target individuals who were identified in the initial request. **If additional individuals become targets of a consensual interception and/or recording in the same investigation, a separate authorization must be obtained for these new targets.**

The following pages have sample official message formats reporting a consensual interception of a non-telephonic communication.

RTF

Sample Official Message for Reporting a Consensual Interception for a Non-Telephonic Communication

FROM:	SAIC-FIELD OFFICE	CASE NUMBER: CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD – APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC – INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF NON-TELEPHONIC COMMUNICATION	
AUTHORIZATION:		(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)
ADVISING AUSA:		(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON THE LEGALITY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)
REASON FOR INTERCEPTION:		(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)
SENSITIVE SITUATION:		(YES OR NO. IF YES, EXPLAIN; SEE " SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER.)
TYPE OF EQUIPMENT USED:		(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)
EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:		
WHETHER OR NOT A RECORDING WAS MADE:		(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)
METHOD OF INSTALLATION:		(ON BODY OF AGENT, ON BODY OF INFORMANT, IN GOVERNMENT VEHICLE, ETC.)
LOCATION WHERE EQUIPMENT WAS USED:		(EXACT STREET ADDRESS, CITY, STATE, JUDICIAL DISTRICT)
NAME OF PERSON(S) INTERCEPTED:		(IDENTIFY PERSON(S) INTERCEPTED, INCLUDE ALL ALIASES, DATES OF BIRTH AND SOCIAL SECURITY NUMBER IF AVAILABLE, OR "UNKNOWN SUBJECT." LIST AUTHORIZED TARGET FIRST, THEN ENTER INCIDENTAL INTERCEPTIONS. LIST EACH SUBJECT BY NUMBER, I.E., 1, 2, ETC.)
NAME OF CONSENTING PARTY:		
DATE OF INTERCEPTION:		
DURATION OF INTERCEPTION:		(STARTING TIME TO ENDING TIME OF THE INTERCEPTION FOR EACH INDIVIDUAL. LIST THE DURATION FOR EACH SUBJECT BY NUMBER AS ABOVE.)
INVESTIGATIVE BENEFITS DERIVED:		(BRIEF SYNOPSIS)
EXPECTED CONTINUED USE:		(YES OR NO).
FIELD OFFICE		CASE SA/SUPERVISOR/SAIC

RIF

Incidental Non-Telephonic Consensual Interception

When a subject other than the target is intercepted, an official message must be sent in the above previously mentioned format or in the following format (see sample below). The message should indicate the authorized target of the interception.

Sample Incidental Non-Telephonic Consensual Interception Official Message (Interception of Non-Target Individuals)

FROM:	SAIC-FIELD OFFICE	CASE NUMBER: CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD – APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC – INVESTIGATIVE SUPPORT DIVISION	
SUBJECT: INTERCEPTION)	CONSENSUAL INTERCEPTION AND OR RECORDING OF NON-TELEPHONIC COMMUNICATION (INCIDENTAL	

ON (DATE), _____ SAIC OF (FIELD OFFICE) AUTHORIZED INTERCEPTION AND RECORDING OF (SUBJECT) PURSUANT TO A COUNTERFEIT INVESTIGATION IN ABOVE CASE NUMBER.

DURING AN ATTEMPT TO LOCATE AND INTERVIEW THE TARGET (NAME), THE FOLLOWING PERSON(S) WAS/WERE INTERCEPTED.

NAME OF PERSON(S) INTERCEPTED:	(IDENTIFY PERSON (S) IF KNOWN. INCLUDE ALL ALIASES, AND IDENTIFIERS, OR UNKNOWN SUBJECT)
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES)
TYPE OF EQUIPMENT USED:	(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)
EQUIPMENT SERIAL AND OR USSS PROPERTY NUMBER:	
WHETHER OR NOT RECORDING MADE:	(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)
METHOD OF INSTALLATION:	(ON BODY OF AGENT, ON BODY OF INFORMANT, ETC.)
LOCATION WHERE EQUIPMENT WAS USED:	(EXACT STREET ADDRESS, CITY, STATE)
NAME OF CONSENTING PARTY:	
DATE OF INTERCEPTION:	
DURATION OF INTERCEPTION:	(START TIME TO END TIME)
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)
EXPECTED CONTINUED USE:	(YES OR NO. IF YES, NOTE HERE IF ADDITIONAL AUTHORIZATION HAS BEEN OR WILL BE REQUESTED)

FIELD OFFICE CASE SA/SUPERVISOR/SAIC

Special Requirements for Sting Operations

"Sting" operation procedures are designed for operations where it is expected that most of the persons to be intercepted would be of the "walk-in" variety, such as in store front operations under conditions where the **target is unknown before he is intercepted**. However, if the "sting" operation is the type where it is known prior to an interception, who is to be intercepted, these blanket authorization procedures do not apply. The normal procedures for obtaining authorization for each target apply.

The reporting requirements for non-telephonic consensual interceptions during a "sting" operation is unique. As in "non-sting" type cases, the field office will provide in advance of the intercept to the appropriate operational division the following information:

1. **Case File Number** (Note: all intercept cases are to be designated as "S" Cases except case classification code 704 "Sting" Operations. Code 704 requires Headquarters distribution of memorandum reports.);
2. **Date of intended use;**
3. **Target to be intercepted;**
4. **Type of violation** (CFT/Financial Crimes/etc.);
5. **Statute violated;**
6. **Office and person making request;**
7. **If sensitive situation (what type?), and**
8. **Name and district of Assistant United States Attorney (AUSA).**

All targets intercepted under this "Blanket Worksheet" will be immediately reported via official message (as in "Non-Sting" cases). Each new target will be assigned a separate case suffix number (first suffix field). Each target can then be intercepted for a sixty day period beginning on the date of the first intercept of that target, without requesting an additional authorization.

Sample "Sting" Operation Official Message

FROM:	SAIC-FIELD OFFICE	CASE NUMBER: CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD – APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC – INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF NON-TELEPHONIC COMMUNICATION - OPERATION (NAME)	
AUTHORIZATION:	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)	
ADVISING AUSA:	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON LEGALITY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)	
REASON FOR INTERCEPTION:	(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)	
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER.)	
TYPE OF EQUIPMENT USED:	(AUDIO/RF TRANSMITTER, RECEIVER, OR RECORDING DEVICES, ETC.)	
EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:		
WHETHER OR NOT RECORDING WAS MADE:	(YES OR NO. IF NO, STATE REASON WHY. I.E., EQUIPMENT FAILURE, ETC.)	
METHOD OF INSTALLATION:	(ON BODY OF AGENT, ON BODY OF INFORMANT, IN GOVERNMENT VEHICLE, ETC.)	
LOCATION WHERE EQUIPMENT WAS USED:	(EXACT STREET ADDRESS, CITY, STATE, JUDICIAL DISTRICT)	
NAME OF PERSON(S) INTERCEPTED:	(IDENTIFY PERSON(S) INTERCEPTED, INCLUDE ALL ALIASES, DATES OF BIRTH AND SOCIAL SECURITY NUMBERS IF AVAILABLE OR "UNKNOWN SUBJECT." LIST AUTHORIZED TARGET FIRST, and THEN ENTER INCIDENTAL INTERCEPTIONS. LIST EACH SUBJECT BY NUMBER, I.E., 1, 2, ETC.)	
NAME OF CONSENTING PARTY:		
DATE OF INTERCEPTION:		
DURATION OF INTERCEPTION:	(STARTING TIME TO ENDING TIME OF THE INTERCEPTION FOR EACH INDIVIDUAL. LIST THE DURATION FOR EACH SUBJECT BY NUMBER AS ABOVE.)	
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS)	
EXPECTED CONTINUED USE:	YES OR NO	
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC	

Reporting of Consensual Telephonic Interception

As with the consensual non-telephonic interception, when conducting a consensual telephonic intercept, an official message must be forwarded to the appropriate operational division with distribution to the appropriate Assistant Director's Office and the Investigative Support Division (ISD). This Official Message should be submitted under the case number of the investigation in which the interception has been conducted. It must be designated special (S) in all cases involving consensual interceptions. The official message should comment on the following factors:

- Name of USSS authorizing official and date of authorization;
- Name of the United States Attorney, Assistant United States Attorney or Organized Crime Strike Force attorney who provided advice as to the legality of the consensual interception, date of advice, and the judicial district to which he/she is assigned;
- Reason for the interception;
- Whether or not the target of the interception falls within any of the six "sensitive" case situations. If yes, explain. (See the six "sensitive" case categories listed in this chapter.);
- Type of equipment used;
- Equipment serial and/or USSS property number;
- Whether or not a recording was made (if no, state reason why, i.e., equipment failure, etc.);
- Method of installation;
- Location where equipment was used (include judicial district);
- Name(s) of all person(s) intercepted, include all aliases, dates of birth, and Social Security numbers if available, or "unknown subject." (The name(s) of the person(s) intercepted for which permission to intercept as a target was obtained should be listed first, and should be denoted as a target);
- Name of consenting party;
- Telephone number to which the call was placed. (If the call was incoming to consenting party, note this in the official message.);
- Telephone number, to include area code from which the call was placed;
- Date of interception;
- Duration of interception;
- Investigative benefits derived. (Be specific if no benefits were derived); and
- Is continued use expected? Yes or No.

Sample Consensual Telephonic Interception Official Message

FROM:	SAIC-FIELD OFFICE	CASE NUMBER: CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD – APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC – INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF TELEPHONIC COMMUNICATION	
AUTHORIZATION:		(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)
ADVISING AUSA:		(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO PROVIDED ADVICE ON LEGALITY OF THE INTERCEPTION. DATE THE ADVICE WAS GIVEN, THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED.)
REASON FOR INTERCEPTION:		(TO OBTAIN INCRIMINATING STATEMENTS, TO CORROBORATE INFORMATION, ETC.)
SENSITIVE SITUATION:		(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER)
TYPE OF EQUIPMENT USED:		(SONY TC-110A TAPE RECORDER, ETC.)
EQUIPMENT SERIAL AND/OR USSS PROPERTY NUMBER:		
WHETHER OR NOT RECORDING WAS MADE:		(YES OR NO)
METHOD OF INSTALLATION:		(INDUCTION COIL, ETC.)
LOCATION WHERE EQUIPMENT WAS USED:		(NAME OF FIELD OFFICE, EXACT STREET ADDRESS, STATE, JUDICIAL DISTRICT)
NAME OF SUBJECT(S) INTERCEPTED:		TARGET(S), (INCLUDE ALL ALIASES, DOB'S, SSN'S, AVAILABLE OR "UNKNOWN")
NAME OF CONSENTING PARTY:		(AGENT NAME, INFORMANT NUMBER, ETC.)
TELEPHONE NUMBER TO WHICH CALL PLACED:		(IF CALL WAS INCOMING TO CONSENTING PARTY, NOTE)
TELEPHONE NUMBER CALL MADE FROM:		
DATE OF INTERCEPTION:		
DURATION OF INTERCEPTION:		(STARTING TIME TO ENDING TIME OF THE INTERCEPTION)
INVESTIGATIVE BENEFITS DERIVED:		(BRIEF SYNOPSIS)
EXPECTED CONTINUED INTERCEPTION:		YES OR NO
FIELD OFFICE		CASE SA/SUPERVISOR/SAIC

Additional Interceptions

A separate official message must be submitted for each and every telephonic and non-telephonic interception.

Interceptions of "Name Unknown" Subjects and Identified Subjects Previously Using an Alias

No additional official messages are necessary when identification is made on subjects using an alias or "unknown subjects." However, the identification will be indicated in the memorandum report referencing the official message which previously reported the target as unknown or subject using an alias.

Telephonic and Non-Telephonic Recordings

Once a recording is made using any type of audio, video, and/or electronic storage device, it must be properly labeled to identify the recording of all consensual interceptions of wire and oral communications. The label must contain the case number, date and time of interception, name of case agent, and person intercepting the communication.

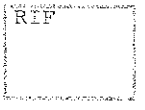
All consensual recordings (audio, video, and/or electronic) will be inventoried on an SSF 1544, Certified Inventory of Evidence, and will be maintained in a secure location. All evidence should be handled in accordance to evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Forensic Services Division (FSD) Homepage, Resources Section.

At the time a non-judicial case is closed, with the approval of the appropriate Headquarters operational division, consensual recordings may be physically destroyed locally. Judicial cases also require permission from the appropriate operational division and consultation with the U.S. Attorney's Office, prior to destruction. **SSF 1544 clearance procedures must be followed when physically destroying consensual recordings. THE AUDIO, VIDEO, AND/OR ELECTRONIC STORAGE DEVICES (TAPES/ DISKS) SHOULD NEVER BE RE-USED FOR THE RECORDING OF EVIDENCE.**

Electronic Communications Consensual Intercepts

As previously stated in this manual, "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronics, or photo-optical system that affects interstate or foreign commerce. Additional reference to this definition and related topics may be found under Title 18 U.S.C. 2510.

Generally speaking, consensual interception of electronic communications over public phone lines or network connection will be handled in the same manner as the interception of telephonic and non-telephonic communication, with the local field office SAIC authorizing the intercept. Prior to the intercept, advice must be obtained from the AUSA as to the legality of the proposed consensual interception.



Examples of consensual computer data transmissions (electronic communications) are as follows:

- Party A communicates with Party B via computer attached by a modem or network connection.
- Party A and Party B communicate with each other directly in what is called the "chat" mode. Typically via an instant messenger program such as ICQ, MSN, AOL, etc.

When two individuals (one consenting-Special Agent/Informant) are communicating over phone lines or network connection using computers, as in the above examples, and the conversation is being recorded, printed or viewed by a third party, a consensual intercept is being made. In these cases an official message must be sent to the appropriate operational division.

NOTE: The private area of an electronic bulletin board is one that does not have general access. An "elite" bulletin board, where there is no general access, is treated the same as the private area of a general access bulletin board. This area, for example, has a special password, not known to the general public. Caution must be exercised when using computer bulletin boards. This type of consensual interception should be thoroughly discussed with the local U.S. Attorney's Office. Prior to an interception, Secret Service personnel may not "hack" onto a bulletin board gaining access by breaking security systems, etc. This would be considered a non-consensual interception and would require a court order.

As in the case of consensual telephonic intercepts, authorization for this type of intercept, conducted over telephone lines or a network connection, should emanate from the SAIC of the investigating field office. The authorization to intercept the electronic communication will be obtained in the beginning of the interception and will be valid for the duration of the investigation. Once an authorization has been given, an official message must be sent every 30 days from the date of initial interception to the appropriate operational division, appropriate AD's office and ISD.

Notification of such intercepts will be made in much the same manner as consensual telephonic intercepts. However, modifications to the official message are necessary. These modifications will include the type of computer equipment used in the intercept in addition to, the property or serial number of the computer equipment.

The intercepted communication must be converted to a hardcopy printout and/or stored to a technologically appropriate storage device. The printouts and or communication stored on a storage device must be treated as evidence and handled in accordance to evidence handling procedures which can be found in the "Reference Guide for "Evid"/Evidence System," located under the Forensic Services Division (FSD) Homepage, Resources Section.

The following page has a sample official message reporting a consensual interception of electronic communication:

Sample Official Message Reporting a Consensual Interception of Electronic Communication

FROM:	SAIC-FIELD OFFICE	CASE NUMBER: CASE TITLE:
TO:	SAIC-APPROPRIATE OPERATIONAL DIVISION	
INFO:	AD – APPROPRIATE ASSISTANT DIRECTORS OFFICE SAIC – INVESTIGATIVE SUPPORT DIVISION	
SUBJECT:	CONSENSUAL INTERCEPTION AND/OR RECORDING OF ELECTRONICS COMMUNICATION	
AUTHORIZATION:	(NAME OF USSS AUTHORIZING OFFICIAL AND DATE OF AUTHORIZATION)	
ADVISING AUSA:	(NAME OF THE ASSISTANT UNITED STATES ATTORNEY WHO HAS GIVEN ADVICE ON LEGALITY OF THE INTERCEPTION, DATE OF ADVICE, AND THE JUDICIAL DISTRICT TO WHICH HE OR SHE IS ASSIGNED)	
REASON FOR INTERCEPTION:	(TO OBTAIN INCRIMINATING STATEMENTS, CORROBORATE INFORMATION, ETC.)	
SENSITIVE SITUATION:	(YES OR NO. IF YES, EXPLAIN; SEE "SIX" SENSITIVE CASE CATEGORIES IN THIS CHAPTER)	
COMPUTER EQUIPMENT USED:	(WITH SERIAL OR USSS PROPERTY #)	
WHETHER OR NOT A COPY WAS MADE:	(YES OR NO. IF NO, STATE REASON WHY, I.E., EQUIPMENT FAILURE, ETC.)	
TYPE OF EQUIPMENT USED TO MAKE COPY:	(WITH SERIAL OR USSS PROPERTY #)	
METHOD OF MAKING COPY:		
NAME OF CONSENTING PARTY:		
NAME OF PERSON BEING INTERCEPTED: (TARGET UNIQUE NETWORK IDENTIFIERS TO INCLUDE TRUE NAME, USERNAME, MAC ADDRESS, NETWORK COMPUTER NAME, PHONE NUMBER, EMAIL ADDRESS, IP ADDRESS, ICQ NUMBER, AIM NUMBER, ETC; LIST THE TARGETS IF THERE IS MORE THAN ONE TARGETS)		
DURATION OF INTERCEPTION:	(MM/DD/CCYY, HH/MM – MM/DD/CC/YY, HH/MM)	
INVESTIGATIVE BENEFITS DERIVED:	(BRIEF SYNOPSIS OF THE INTERCEPTION RESULT)	
EXPECTED CONTINUED INTERCEPTION:	YES OR NO	
FIELD OFFICE	CASE SA/SUPERVISOR/SAIC	

RIF

Reports to the Department of Justice (DOJ)

There are no reporting requirements to the Attorney General for consensual monitoring. However, the Department of Justice requires an agency to maintain the records of all consensual monitoring. The Investigative Support Division will maintain all the consensual monitors approved and conducted for three (3) years, per General Records Schedule 23.