9-7.000
ELECTRONIC SURVEILLANCE

9-7.010 Introduction

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders -- Overview and History of Legislation

9-7.110 Format for the Authorization Request

9-7.111 Roving Interception

9-7.112 Emergency Interception

9-7.200 Video Surveillance -- Closed Circuit Television -- Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

9-7.250 Use and Unsealing of Title III Affidavits

9-7.301 Consensual Monitoring -- General Use

9-7.302 Consensual Monitoring -- "Procedures for Lawful, Warrantless Interceptions of Verbal Communications"

9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings

9-7.010

Introduction

This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, *et seq*. Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information concerning use of the various types of electronic surveillance is also set forth in the Criminal Resource Manual at 27.

Attorneys in the Electronic Surveillance Unit of the Office of Enforcement Operations, Criminal Division, are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. Interceptions conducted pursuant to the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, *et seq.*, are specifically excluded from the coverage of Title III. *See* 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders -- Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted. Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. *See, e.g., Katz v. United States*, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State law in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at USAM 9-7.111.)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. Electronic communications are those types of non-oral or wire communications that occur, *inter alia*, over computers, digital-display pagers, and facsimile ("fax") machines. *See* 18 U.S.C. § 2510(12).

Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of electronic communications over any other device, such as computers and fax machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers--which are the most commonly targeted type of electronic communications--may be made based solely upon the authorization of a United States Attorney. *See* 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. *See* 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.

See the Criminal Resource Manual at 31, for citations to relevant legislation.

9-7.110 Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;

B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and

C. A set of orders to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application, including appropriate redacted orders to be served on any relevant providers of "electronic communication service" (as defined in 18 U.S.C. § 2510(15)).

9-7.111 Roving Interception

Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. *See United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *cert. denied*, 114 S. Ct. 1644 (1994); *United States v. Orena*,

883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications will be intercepted when it can be shown that the subject or subjects of the interception have demonstrated a purpose to thwart interception by changing facilities. *See United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), *cert. denied*, 113 S.Ct. 1859 (1993); *United States v. Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993).

When the government seeks authorization for roving interception, the Department's authorization must be made by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an Acting Assistant Attorney General. *See* 18 U.S.C. § 2518(11)(a)(i) and (b)(i).

9-7.112 Emergency Interception

Title III contains a provision which allows for the warrantless, emergency interception of wire, oral, and/or electronic communications. Specifically, under 18 U.S.C. § 2518(7), the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AssocAG) may specially designate a law enforcement or investigative officer to determine whether an emergency situation exists that requires the interception of wire, oral, and/or electronic communications before a court order authorizing such interception can, with due diligence, be obtained. As defined by 18 U.S.C. § 2518(7), an emergency situation involves either: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities threatening the national security interest; or (3) conspiratorial activities characteristic of organized crime. The only situations which will likely constitute an emergency are those involving an imminent threat to life, i.e., a kidnapping or hostage taking. *See United States v. Crouch*, 666 F. Supp. 1414 (N.D. Cal. 1987)(wiretap evidence suppressed because there was no imminent threat of death or serious injury); *Nabozny v. Marshall*, 781 F.2d 83 (6th Cir.)(kidnapping and extortion scenario constituted an emergency situation), *cert. denied*, 476 U.S. 1161 (1986). The emergency provision also requires that grounds must exist under which an order could be entered (*viz*., probable cause, necessity, specificity of target location/facility) to authorize the interception. Once the AG, the DAG, or the AssocAG authorizes the law enforcement agency to proceed with the emergency Title III, the government then has forty-eight (48) hours, from the time the authorization was granted, to obtain a court order approving the emergency interception. 18 U.S.C. § 2518(7). The affidavit supporting the application for the order must contain only those facts known to the AG, the DAG, or the AssocAG at the time his or her approval was given, and must be accompanied by a written verification from the requesting agency noting the date and time of the authorization. Failure to obtain the court order within the forty-eight-hour period will render any interceptions obtained during the emergency illegal.

Prior to the agency's contact with the AG, the DAG, or the AssocAG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the Office of Enforcement Operation's Electronic Surveillance Unit, which is the initial contact for the requesting United States Attorney's Office and the requesting agency. Once the Electronic Surveillance Unit attorney briefs and obtains oral approval from the AAG or the DAAG, the attorney notifies the agency representative and the Assistant United States Attorney that the Criminal Division recommends that the emergency authorization proceed. The agency then contacts the AG, the DAG, or the AssocAG and seeks permission to proceed with the emergency Title III.

9-7.200 Video Surveillance -- Closed Circuit Television -- Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

Pursuant to Department of Justice Order No. 985-82, dated August 6, 1982, certain officials of the Criminal Division have been delegated authority to review requests to use video surveillance for law enforcement purposes when there is a constitutionally protected expectation of privacy requiring judicial authorization. This authority was delegated to the Assistant Attorney General, any Deputy Assistant Attorney General, and the Director and Associate Directors of the Office of Enforcement Operations.

When court authorization for video surveillance is deemed necessary, it should be obtained by way of an application and order predicated on Fed. R. Crim. P. 41(b) and the All Writs Act (28 U.S.C. § 1651). The application and order should be based on an affidavit that establishes probable cause to believe that evidence of a Federal crime will be obtained by the surveillance. In addition, the affidavit should comply with certain

provisions of the Federal electronic surveillance statutes. See the Criminal Resource Manual at 32 for additional discussion of video surveillance warrants.

Department policy requires that the video surveillance application and order be filed separately from, and not incorporated in, an application and order for electronic surveillance pursuant to 18 U.S.C. § 2518. When appropriate, the same affidavit may be submitted in support of both applications/orders.

9-7.250 Use and Unsealing of Title III Affidavits

When the government terminates a Title III electronic surveillance investigation, it must maintain under seal all of the Title III applications and orders (including affidavits and accompanying material) that were filed in support of the electronic surveillance. *See* 18 U.S.C. § 2518(8)(b); *In re Grand Jury Proceedings*, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988) (although 18 U.S.C. § 2518(8)(b) refers only to "applications" and "orders," "applications" is construed to include affidavits and any other related documentation).

The purpose of this sealing requirement is to ensure the integrity of the Title III materials and to protect the privacy rights of those individuals implicated in the Title III investigation. *See* S.Rep. No. 1097, *reprinted in* 1968 U.S. Code Cong. & Admin. News 2112, 2193-2194. The applications may be unsealed only pursuant to a court order and only upon a showing of good cause under 18 U.S.C. § 2518(8)(b) or in the interest of justice under 18 U.S.C. § 2518(8)(d).

Thus, the government attorney should not attach Title III affidavits or other application material as exhibits to any search warrant affidavit, complaint, indictment, or trial brief. The government attorney may, nevertheless, use information from these materials or the Title III interceptions in documents such as search warrant affidavits, complaints, indictments, and trial briefs. *See* 18 U.S.C. § 2517(8)(a); 18 U.S.C. § 2517(1) and (2); and S.Rep. No. 1097 at 2188. In using this information, however, the government attorney must use care not to disclose publicly information from the Title III affidavits or interceptions that would either abridge the privacy interests of persons not charged with any crime or jeopardize ongoing investigations.

When Title III materials are sought by defense counsel or other persons and the privacy interests of uncharged persons are implicated by the contents of those materials, the government attorney should seek a protective order pursuant to Rule 16(d)(1), Fed. R. Crim. P., that will forbid public disclosure of the contents of the materials. Likewise, a Rule 16 protective order should be sought to deny or defer discovery of those portions of the affidavits and applications that reveal ongoing investigations when disclosure would jeopardize the success of any such investigation.

For discussion about disclosure of intercepted communications in civil litigation see the Criminal Resource Manual at 33-34.

9-7.301 Consensual Monitoring -- General Use

Section 2511(2)(c) of Title 18 provides 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...." *See United States v. White*, 401 U.S. 745 (1971). As such, consensual interceptions need not be made under Title III procedures, interception orders under § 2518 are not available, and should not be sought in cases falling within § 2511(2)(c).

The Fourth Amendment to the U.S. Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, *et seq.*), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, *et seq.*) permit government agents, acting

with the consent of a party to a communication, to engage in warrantless interceptions of telephone communications, as well as oral and electronic communications. *White*, *supra*; *United States v. Caceres*, 440 U.S. 741 (1979). Similarly, Title III, by its definition of oral communications, permits Federal agents to engage in warrantless interceptions of oral communications when the communicating parties have no justifiable expectation of privacy. 18 U.S.C. § 2510(2). (No similar exception is contained in the definition of wire communications and, therefore, the nonconsensual interception of wire communications violates 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court authorization procedures of Title III or with the provisions of the Foreign Intelligence Surveillance Act of 1978.) Since such interception techniques are particularly effective and reliable, the Department of Justice encourages their use by Federal agents for the purpose of gathering evidence of violations of Federal law, protecting the safety of informants and undercover law enforcement agents, or fulfilling other compelling needs. While these techniques are lawful and helpful, their use is frequently sensitive, so they must remain the subject of careful self-regulation by the agencies employing them.

The Department developed guidelines for the investigative use of consensual monitoring, which were promulgated most recently by the Attorney General on November 7, 1983. The guidelines do not apply to consensual monitoring of telephone conversations or radio transmissions. It was left to the enforcement agencies to develop adequate internal guidelines for the use of those aspects of this investigative tool. The following guidelines cover the investigative use of devices which intercept and record certain consensual verbal conversations where a body transmitter or recorder or a fixed location transmitter or recorder is used during a face-to-face conversation. In certain specified sensitive situations, under the regulations, the agencies must obtain advance written authorization from the Department of Justice. (Efforts have been ongoing within the Department to modify these guidelines, including limiting the "sensitive circumstances" under which Department approval is required; however, the 1983 guidelines remain the current Department policy.) The guidelines on consensual monitoring set forth in the Attorney General's Memorandum of November 7, 1983, on that subject are contained in USAM 9-7.302.

9-7.302 Consensual Monitoring -- "Procedures for Lawful, Warrantless Interceptions of Verbal Communications"

The following text was taken from a memorandum on "Procedures for Lawful, Warrantless Interceptions of Verbal Communications" issued by the Attorney General on November 7, 1983:

I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies and specifically includes United States Attorneys' offices which utilize their own investigators and the Offices of the Inspectors General.

As used in this Memorandum, the term "interception" means the aural acquisition of verbal communications by use of an electronic, mechanical, or other device. *Cf.* 18 U.S.C. § 2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts as well as all federal, state, county, and municipal governmental units.

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required. A request for authorization to intercept a verbal communication without the consent of all parties to the communication must be sent for approval to the Director of the Office of Enforcement Operations, Criminal Division, Department of Justice, when it is known that:

(1) The interception relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV, or above, or a person who has served in such capacity within the previous two years;

(2) The interception relates to an investigation of any public official and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) The interception relates to an investigation of a federal law enforcement official;

(4) The consenting or nonconsenting person is a member of the diplomatic corps of a foreign country;

(5) The consenting or nonconsenting person is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(6) The consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(7) The Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent for making a consensual interception in a specific investigation.

B. Investigations Where Written Department of Justice Approval is Not Required. In all other cases approval of consensual surveillances will be in accordance with the procedures set forth in Part V below.

C. Interceptions Not Within Scope of Memorandum. Even if the interception falls within one of the seven categories above, the procedures and rules do not apply to:

(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.*) (Refer to FISA procedures);

(3) Interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, *et seq.*) (Refer to Title III authorization procedures);

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

(5) Consensual interceptions of radio communications; and

(6) Consensual interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information. Where a request to DOJ is required, as set forth in the above paragraphs, the following information must be set forth on any request to intercept a verbal communication without the consent of all parties to the communication:

(1) Reasons for the Interception. The request must contain a reasonably detailed statement of the background and need for the interception.

(2) Offense(s). If an interception is for investigative purposes, the request must include a citation to the principal criminal statute(s) involved.

(3) Danger. If an interception is for protection purposes, the request must explain the danger to the consenting party or other persons.

(4) Location of Devices. The request must state where the interception device will be hidden, i.e. , on the person, in personal effects, or in a fixed location.

(5) Location of Interception. The request must specify the location and primary judicial district where the interception will take place. An interception authorization is not restricted to the original district. However, if the location of an interception changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.

(6) Time. The request must state the length of time needed for the interception. Initially, an authorization may be granted for up to thirty days from the day the interception is scheduled to begin. If there is need for continued interception, extensions for periods of up to thirty days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents), authorization for up to sixty days may be granted with similar extensions.

(7) Names. The request must give the names of persons, if known, whose communications the department or agency expects to intercept and the relation of such persons to the matter under investigation or to the need for the interception.

(8) Trial Attorney Approval. The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, an Organized Crime Strike Force Attorney for the district in which the surveillance will occur, or any previously designated Department of Justice attorney for a particular investigation, and that such attorney has stated that the surveillance is appropriate under this Order. Such statement may be made orally.

(9) Renewals. A request for renewed authority to intercept verbal communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed.

B. Verbal Requests. Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency (for example, telephonic) requests in cases in which written Department of Justice approval is required may be made to the Director or Associate Director of the Office of Enforcement Operations and should then be reduced to writing and submitted to the appropriate headquarters official as soon as possible after authorization has been obtained. An appropriate headquarters filing system is to be maintained for surveillance requests which have been received and approved in this manner. These verbal requests must include all the information required for any regular written requests as set forth above.

C. Authorization. Authority to engage in a consensual interception in situations set forth in Part II, A above may be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General in charge of the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or Associate Director of the Criminal Division's Office of Enforcement Operations.

D. Emergency Interceptions. If an emergency situation requires a consensual interception during non-working hours at the Department of Justice, the authorization may be given by the head of the responsible department or agency, or his or her designee. Such department or agency must then notify the Office of Enforcement Operations not later than five working days after the emergency authorization. The notification shall explain the emergency and shall contain all other items required for a non-emergency request for authorization as set forth in Part III, A above.

IV. SPECIAL LIMITATIONS

A. Consensual Interceptions. When a communicating party consents to the interception of his or her verbal communications, the device may be concealed on his or her person, in personal effects, or in a fixed location. Each department and agency engaging in such consensual interceptions must ensure that the consenting party will

be present at all times when the device is operating. In addition, each department and agency must ensure: (1) that no agent or person cooperating with the department or agency trespasses while installing a device in a fixed location, and (2) that as long as the device is installed in the fixed location, the premises remain under the control of the government or of the consenting party. *See United States v. Padilla*, 520 F.2d 526 (1st Cir. 1975).

B. Non-Consensual, Non-Private Interceptions. The interceptions of verbal, non-wire communications when no party to the communication has consented and when no party has a justifiable expectation of privacy must be conducted under tightly controlled circumstances. (For example, burglars, while committing a burglary, have no justifiable expectation of privacy. *Cf. United States v. Pui Kan Lam*, 483 F.2d 1202 (2d Cir. 1973), *cert. denied*, 415 U.S. 984 (1974).) Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted.

V. CONSENSUAL INTERCEPTIONS WHERE NO WRITTEN APPROVAL REQUIRED

Each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual interceptions of verbal communications. Approval for a consensual interception must come from the head of the agency or his/her designee. Any designee should be a high-ranking supervisory official at headquarters level. Prior to receiving approval for a consensual interception from the head of the agency or his/her designee, a representative of the agency must contact the United States Attorney, an Assistant United States Attorney, an Organized Crime Strike Force attorney in the district where the interception is to occur, or any previously designated Department of Justice attorney for a particular investigation. Final authorization may be obtained verbally from the attorney so contacted. The attorney, in giving final authorization, will determine both the legality and propriety of the interception in question.

Each department or agency shall establish procedures for emergency authorizations consistent with the requirements of

Part III, D above, with a follow-up verbal Department of Justice attorney authorization.

Records are to be maintained for each interception. These records are to include the information set forth in items 1 through 8 of Part III, A above.

VI. REPORTS

The head of each department or agency, or his or her designee, shall make quarterly reports summarizing the results of interceptions authorized pursuant to this Memorandum. The report shall contain the following information broken down by offense or reason for interception: the number of requests for authorization, the number of emergency authorizations, the number of times that the interceptions provided information which corroborated or assisted in corroborating the allegation or suspicion, and the number of authorizations not used. The quarterly reports shall be submitted in January, April, July,

and October of each year to the Office of Enforcement Operations in the Criminal Division.

In October of each year, each department or agency shall submit to the Attorney General an inventory of all devices which are intended for the surreptitious interception of telephone or verbal, non-wire communications, including devices used to intercept communications pursuant to the warrant provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986.

VII. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual interception of verbal communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual interception.

9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings

See the Criminal Resource Manual at 35, for a discussion of the law related to disclosure of defendant overhearings and attorney overhearings.