DoD O-5505.9-M

Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement

May 1995

Inspector General of the Department of Defense

FOR OFFICIAL USE ONLY

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

FOREWORD

This Manual is issued under the authority of DoD Directive 5505.9, "Interception of Wire, Electronic, and Oral Communications for Law Enforcement," April 20, 1995. It provides procedures for requesting and approving law enforcement intercepts; specifies reporting requirements and formats; and provides guidance on storage, retention, and disposal of interception equipment.

This Manual applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). This Manual is effective immediately.

Send recommended changes to the Manual to:

Assistant Inspector General, Criminal
Investigative Policy and Oversight
400 Army Navy Drive, Room 1037
Arlington, VA 22202-2884

The DoD Components may obtain copies of this Manual through their own publications channels. This Manual contains information concerning law enforcement methods and techniques and shall not be released to the public.

Eleanor Hill
Inspector General

TABLE OF CONTENTS

FIGURES

REFERENCES

(a) Sections 2510-2520, 2701-2711, and 3121-3127 of title 18, United States Code
b) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 25, 1988
Chapter 47 of title 10, United States Code, "Uniform Code of Military Justice (UCMJ)"
(d) U.S. Constitution, Amendment 4
(e) DoD Directive 5505.9, "Interception of Wire, Electronic, and Oral Communications for Law Enforcement," April 20, 1995
Public Law 93-579, "Privacy Act of 1974," December 31, 1974, as amended (5 U.S.C. 552a)
DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
Public Law 89-554, "Freedom of Information Act of 1967," September 6, 1966, as amended (5 U.S.C. 552)
DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988

DEFINITIONS

1. Aural Transfer. A transfer containing the human voice at any point between and including the point of origin and the point of reception (Subsection 2510(18) of 18 U.S.C., reference (a)).

2. Consensual Interception. An interception by a person acting under color of law of a wire, oral, or electronic communication where such party is a party to the communication or one of the parties to the communication has given prior consent to such interception (Subsection 2511(2)(c) of 18 U.S.C., reference (a))

3. Contents. When used about any wire, oral, or electronic communication, includes any information on the substance, purport, or meaning of that communication (Subsection 2510(8) of 18 U.S.C., reference (a)).

4. Counterintelligence. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons, or international terrorist activities, but not including personnel, physical, document, or communications security programs under DoD 5240.1-R (reference (b)).

5. Defense Criminal Investigative Organizations (DCIOs). Includes the U.S. Army Criminal Investigation Command, the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the Defense Criminal Investigative Service.

6. DoD Personnel. Civilian employees of the Department of Defense, active and Reserve duty members of the Military Services, retired members of the Military Services, and dependents of civilian employees and active duty members.

7. Electronic Communication. Any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects the interstate or foreign commerce (Subsection 2510(12) of 18 U.S.C., reference (a)), but does not include:

a. The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

b. Any wire or oral communication

c. Any communication made through a tone-only paging device.

d. Any communication from a tracking device as defined in 18 U.S.C. Section 3117 (reference (a)).

8. Electronic Communication Service. Any service that provides to users thereof the ability to send or receive wire or electronic communications (Subsection 2510(15) of 18 U.S.C., reference (a)).

9. Electronic, Mechanical, or other Device. Any device or apparatus that can be used to intercept a wire, oral, or electronic communication other than:

a. Any telephone or telegraph instrument, equipment, or facility, or any component thereof, as follows:

(1) Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business;

(2) Furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or

(3) Being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his or her duties; and

b. A hearing aid or similar device being used to correct subnormal hearing to not better than normal (Subsection 2510(5) of 18 U.S.C., reference (a)).

10. Electronic Storage

a. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

b. Any storage of such communication by an electronic communication service for backup protection of such communication (Subsection 2510(17) of 18 U.S.C., reference (a)).

11. Foreign Intelligence. Information on the capabilities, intentions, and activities of foreign powers, organizations, or persons, including information on the foreign aspects of narcotics production and trafficking, but not including counterintelligence, except for information on international terrorist activities under reference (b).

12. Intercept. The aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device (Subsection 2510(4) of 18 U.S.C., reference (a)).

13. Oral Communication. Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication (Subsection 2510(2) of 18 U.S.C., reference (a)).

14. Pen Register. A device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. The term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communication services provided by such provider, or any device used by a provider or customer of a wire communication service for cost accounting, or other similar purposes in the ordinary course of its business (Subsection 3127(3) of 18 U.S.C., reference (a)).

15. Public Official. An official of any public entity of the Government, including special districts, Federal, State, county, and municipal governmental units (Appendix A, page A-3).

16. Remote Computing Service. The provision to the public of computer storage or processing services by means of an electronic communications system (Subsection 2711(2) of 18 U.S.C., reference (a)).

17. Trap and Trace Device. A device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted (Subsection 3127(4) of 18 U.S.C., reference (a)).

18. User. Any person or entity who:

a. Uses an electronic communication service; and

b. Is duly authorized by the provider of such service to engage in such use (Subsection 2510(13) of 18 U.S.C., reference (a)).

19. Wire Communication. Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. The term includes any electronic storage of such communication, but does not include the radio portion of a

cordless telephone communication that is transmitted between the cordless telephone handset and the base unit (Subsection 2510(1) of 18 U.S.C., reference (a)).

ABBREVIATIONS AND/OR ACRONYMS

1.	CONUS	Continental United States
2.	DCIOs	Defense Criminal Investigative Organizations
3.	DPS	Defense Protective Service
4.	GC	General Counsel
5.	IG	Inspector General
6.	OCONUS	Outside CONUS
7.	OEO, DoJ	Office of Enforcement Operations, Department of Justice
8.	RCS	Report Control Symbol
9.	SOFA	Status of Forces Agreement
10.	UCMJ	Uniform Code of Military Justice
11.	U.S.	United States
12.	U.S.C.	United States Code

CHAPTER 1

PROCEDURES GOVERNING INTERCEPTION OF WIRE, ELECTRONIC, AND ORAL COMMUNICATIONS, PEN REGISTERS, AND TRAP AND TRACE DEVICE OPERATIONS FOR LAW ENFORCEMENT

A. CONSENSUAL INTERCEPTS

1. Applicability. This section governs the DCIOs and the DPS, which intercept wire, electronic, and oral communications, and the audio portion of a video monitoring, for law enforcement when at least one party to the communication has given consent, in and outside the United States, except as follows:

a. A DCIO or the DPS may employ consensual monitoring techniques without DoD approval based on approvals granted to or obtained by another Federal law enforcement agency with which it is engaged in a joint investigation. Each DoD Component may implement supplemental approval procedures when DoD personnel participate in the monitoring, when DoD equipment is used in the monitoring, or when the monitoring takes place on a military installation.

b. Law enforcement personnel of the Department of Defense are authorized to monitor telephone conversations for law enforcement by use of an existing extension telephone instrument, with the consent of at least one party to the conversation, without prior approval.

2. Procedures

a. Except as noted in subsection A.1., above, consensual interceptions of wire, electronic, or oral communications shall be approved in writing by the Secretaries of the Military Departments, or their designees, by the IG, DoD, or designee, or by the Director, Washington Headquarters Services, before such interception is conducted, except in emergency situations. The approval authority shall not be delegated to an official below the head of the DCIO. Each request shall be reviewed for legal sufficiency before its approval.

b. Requests for consensual interception of wire, electronic, or oral communication shall provide the following:

(1) A reasonably detailed statement of the background and need for the interception and the nature of the evidence sought.

(2) A citation of the applicable Federal, State, foreign statute, or provision of the Uniform Code of Military Justice (UCMJ) (reference (c)).

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

(4) A general description of the type(s) of device(s) to be used and their location; i.e., on the person, in personal effects, or in a fixed location.

(5) A particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted. In the United States, the request must include reference to the primary judicial district where the interception will take place for targets not subject to the UCMJ (reference (c)), or the convening authority for targets subject to the UCMJ.

(6) The length of time needed for the interception. Initially, an authorization may be granted for up to 30 days from the day the interception is scheduled to begin. Extensions for periods of up to 30 days may be granted. In special cases, such as targeted narcotics sales sites, fencing or undercover operations, authorization for up to 60 days may be granted with similar extensions. (See the Appendix A, paragraph III.A.(6).)

(7) The name of the consenting party. Names of undercover operatives, cooperating citizens, or informants may be identified by an individualized informant or source control number. If consent was not obtained in writing, submit a statement explaining how consent was obtained.

(8) Names, when known, of nonconsenting parties whose conversations are expected to be intercepted, or who are otherwise to be monitored, and their roles in the offense being investigated.

(9) A statement that the facts of the interception have been discussed with the cognizant prosecuting attorney and that such attorney has indicated (orally or in writing) the interception is appropriate. If the target of the investigation is subject to the UCMJ (reference (c)), the statement of facts shall be discussed with and approved by a judge advocate with the appropriate functional responsibilities.

(10) A request for renewal authority 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.

c. Written authorization from Office of Enforcement Operations, Department of Justice (OEO, DoJ), shall be obtained 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 2 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 pertaining 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 U.S. Marshals Service; or

(7) The Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General for the Criminal Division, or the U.S. Attorney for the district where an investigation is being conducted has requested the investigating Agency obtain prior written consent for making a consensual interception in a specific investigation (Appendix A, subsection II.A.).

d. Subject to additional requirements if subsection III.D. of Appendix A becomes applicable, emergency authorization to conduct a consensual intercept for a period not to exceed 10 days may be granted orally when it is not possible to process a written application because of the following:

(1) Significant new information must be acted on before written authorization can be obtained;

(2) A person's life or physical safety is reasonably believed to be in immediate danger;

(3) The physical security of a DoD installation or other significant U.S. Government property is reasonably believed to be in immediate danger, or evidence of significant criminal conduct is likely to be lost before the written application can be processed; or

(4) The security or execution of a U.S. military operation is threatened or the security interests of the United States are otherwise jeopardized.

e. Within 48 hours after oral authority to conduct an emergency consensual intercept has been granted, the requesting

or higher element shall prepare for the authorizing official a document explaining the emergency and containing all other items required in paragraph A.2.b. of this Chapter, above. When written authorization from the DoJ would have been required under paragraph A.2.c. of this Chapter, above, the document shall be sent to the OEO, DoJ, not later than 5 working days after the emergency authorization is granted.

f. Consensual interception of wire, electronic, or oral communications conducted outside the United States shall also include a statement that the interception is not prohibited by foreign law, Status of Forces Agreement (SOFA), or other agreement with host country authorities.

B. NONCONSENSUAL INTERCEPTIONS

1. In the United States. Except as permitted in subsection B.3. of this Chapter, below, nonconsensual interception in the United States of wire, electronic, and oral communications, and the audio portion of a video monitoring for law enforcement is permitted only after a court order has been obtained, in accordance with 18 U.S.C. 2518 (reference (a)), and only for the offenses enumerated in Section 2516 of reference (a). The Secretaries of the Military Departments, or their designees, or the IG, DoD, or designee, in accordance with procedures adopted by each such organization, may directly request of the appropriate authority the preparation and presentation of the application for a court order to proper judicial authority. The DCIO shall provide such assistance to the requesting authority, as may be required.

2. Outside the United States

a. When the target of the law enforcement investigation is subject to the UCMJ ((reference (c)), the following shall apply:

(1) Application for an authorization may be submitted to a neutral and detached officer who also serves as a military judge designated for that purpose by the Judge Advocate General of the Military Department concerned, in accordance with procedures established by the Secretaries of the Military Departments, or their designees.

(2) Applications for authorizations to be issued by military judges shall contain the information required by 18 U.S.C. 2518(1) (reference (a)).

(3) The military judge may enter an ex parte authorization, as requested or modified, authorizing or approving an interception of wire, electronic, or oral communications by the DCIO concerned, if, on the basis of the application submitted

and other information provided by the requesting Agency, the judge determines that:

(a) There is probable cause to believe that a person subject to the UCMJ ((reference (c)), is committing, has committed, or is about to commit any offense enumerated in 18 U.S.C. 2516(1) and 2516(2) (reference (a)) and analogous UCMJ ((reference (c)) offenses, including any conspiracy to commit any of the listed offenses.

(b) There is probable cause to believe that particular communications about 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 Section 2518(11) of reference (a), there is probable cause to believe that the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted are being, or are about to be, used for the commission of the offense under investigation, or are leased to, listed in the name of, or commonly used by, a person subject to the UCMJ (reference (c)).

(e) The interception does not violate foreign law, any applicable SOFA, or other agreement with host country authorities.

(4) Each authorization of the interception shall comply with the requirements of Subsections 2518(4) and 2518(5) of 18 U.S.C. (reference (a)), to the extent such requirements do not exceed the authority of the official issuing the authorization. Extensions of an authorization may be granted in accordance with Subsection 2518(5) of reference (a).

b. When the target of the law enforcement investigation is not subject to the UCMJ ((reference (c)), nonconsensual interceptions of wire, electronic, and oral communications are permitted only in accordance with host country laws, any applicable SOFA, and any other agreement with the host country. The investigative component shall ensure that the target's rights, as applicable, under the 4th amendment to the U.S. Constitution (reference (d)) are not infringed.

3. When an emergency situation, as described in 18 U.S.C. 2518(7)(a) (reference (a)), exists and there is not sufficient time to obtain an authorization, the Head of the DoD Component concerned may authorize interception of a wire, electronic, or oral communication. The Head of the DoD Component concerned shall, within 48 hours after the interception occurs or begins to

occur, notify the OEO, DoJ, which shall seek the authorization of the Attorney General for the nonconsensual interception.

C. ACCESS TO ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE OR IN A REMOTE COMPUTING SERVICE; RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE

1. Applicability. Subsections C.2. through C.4. of this Chapter, below, govern access to electronic communications in electronic storage or in a remote computing service, and records concerning electronic communication services or remote computing services obtained by the DoD Components for law enforcement in the United States in accordance with Section 2703 of 18 U.S.C. (reference (a)). This section does not apply to Government-owned and -operated computer networks not providing services to the public.

2. Electronic Communications Held in Electronic Storage

a. Access to the contents of an electronic communication held in electronic storage for 180 days or less is permitted only pursuant to a warrant issued under the Federal rules of criminal procedure or equivalent State warrant.

b. Access to the contents of an electronic communication held in electronic storage for more than 180 days shall be obtained in accordance with the procedures in paragraph C.3.a. of this Chapter, below.

3. Electronic Communications Held in a Remote Computing Service. Access to the contents of an electronic communication held in or maintained by a remote computing service shall be obtained as follows:

a. When notice is not given to the subscriber or customer of the remote computing service, a warrant shall be obtained as described in paragraph C.2.a. of this Chapter, above.

b. When notice is provided to the subscriber or customer of the remote computing service, access may be obtained by administrative subpoena (e.g., IG, DoD, subpoena) authorized by a Federal or State statute, Federal or State grand jury or trial subpoena, or by court order.

4. Records Concerning Electronic Communication Service or Remote Computing Service. Access to records or other information about a subscriber or customer of an electronic communication service or remote computing service not including the contents of communications covered by subsections C.2. and C.3. of this Chapter, above, may be obtained in the following ways:

a. By administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;

b. By warrant, as described in paragraph C.2.a. of this Chapter, above;

c. By court order under Section 2703(d) of reference a) and paragraph C.2.a. of this Chapter, above; or

d. With the consent of the subscriber or customer.

D. PEN REGISTERS AND TRAP AND TRACE DEVICES

1. In the United States

a. Except when the consent of the user has been obtained, the installation and use of a pen register or trap and trace device (including "caller ID" units) is permitted only after a court order has been obtained, in accordance with Sections 3122-3123 of 18 U.S.C. (reference (a)). Notice to all users that a device is to be installed on electronic communication lines located on DoD installations or under DoD jurisdiction shall be construed as user consent. If notice to all users is not given because it would result in an undesired effect on the investigation (e.g., it would alert a target of the fact of an investigation), a court order must be obtained.

b. Where the consent of the service user has not been obtained, the following procedures shall be used to obtain authorization to use and install a pen register or trap and trace device:

(1) An attorney from the local U.S. Attorney's Office or from the Department of Justice shall make application for an order, or an extension of an order, authorizing or approving the installation and use of a pen register or trap and trace device, in writing, under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) The application shall include the identity of the attorney making the application, the identity of the law enforcement Agency conducting the investigation, and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that Agency.

(3) Emergency authorization to use and install a pen register or trap and trace device shall be requested in accordance with 18 U.S.C. 3125 (reference (a)) through coordination with the local U.S. Attorney or the OEO, DoJ.

2. Outside the United States

a. If the target of the law enforcement investigation is subject to the UCMJ ((reference (c)), and trial by court-martial may result, before an order may be issued, a military judge assigned to receive such application by the Judge Advocate General, pursuant to subsection E.5. of DoD Directive 5505.9 (reference (e)), must find that the contemplated use and installation of a pen register or trap and trace device does not violate the law of the host country, any applicable SOFA, or any other agreement with the host country. In addition, the procedures and requirements of paragraph D.1.a. and subparagraph D.1.b.(2) of this Chapter, above, must also be met.

b. The Secretaries of the Military Departments may establish procedures for emergency authorization of operations. The approval authority must remain at the General Court Martial Convening Authority or higher.

c. If the target of the law enforcement investigation is not subject to the UCMJ ((reference (c)) and prosecution in the United States is not anticipated, use and installation of such devices is permitted only in accordance with the laws of the host country, any applicable SOFA, or any other agreement with the host country.

CHAPTER 2

RECORDS ADMINISTRATION AND REPORTING REQUIREMENTS

A. GENERAL

All requests for, authorizations or denials of, and recordings and records of information obtained through interception activities accomplished under Chapter 1 shall be retained and safeguarded to prevent unauthorized access, theft, or use. The interest of the Government and the rights of private individuals shall be considered in development of safeguarding procedures.

B. RECORDS REQUIREMENTS

1. Interceptions. Indices of all consensual and nonconsensual interceptions authorized under sections A. and B of Chapter 1 shall be prepared and maintained to provide for centralized, readily accessible, and retrievable records, to include the following elements:

a. Name, citizenship, and other available identifying data for each "reasonably identifiable person" intercepted (intentionally or otherwise), whether a case subject or not. If available, the Social Security number and date and place of birth of the individuals intercepted and identified. Excluded from the requirement are identifying data of special agents, undercover operatives, informants, police, and law enforcement personnel. Special agents, undercover operatives, informants, police and law enforcement personnel who were targeted as suspects should be indexed.

b. Known telephone numbers or radio telephone call signs involved in each interception.

c. Case number or other identifier for each interception.

d. Address of the location of each interception. The address should be sufficiently specific to identify uniquely the location. Extent of detail may vary depending on the locale involved.

e. Inclusive dates of each interception (not dates authorized).

2. Denied Interception Applications. Records of all applications submitted to and disapproved by a Federal or military judge for authorization for a nonconsensual interception of a wire, electronic, or oral communication shall be prepared and maintained in a separate and centralized index that shall include the following information:

a. Name and other available identifying data for each reasonably identifiable target of the applied for interception.

b. Telephone numbers or radio telephone call signs involved in the application.

c. Address(es) of the location of the interception applied for.

d. Case number or other identifier for the application.

e. Statement of the other facts about the application and the reason the application was refused. (For the purposes of subsection B.3. of this Chapter, below, provide a brief explanation of why the interception was not done.)

3. Approved, But Not Done. Indexing data required by subsection B.2. of this Chapter, above, shall be retained in those instances where interception was authorized, but was not done.

4. Retention. Data indexed shall be retained in accordance with the investigative records retention procedures of the DoD Component.

C. DISSEMINATION CONTROLS

1. The index and records maintained under subsection B.1. of this Chapter, above, shall be used only as required to satisfy the requirements of Subsections 2517 and 2518(1)(e) of 18 U.S.C. (reference (a)), this Chapter, and Chapter 3.

2. In all cases, access to information obtained by interception activities conducted under Chapter 1 shall be restricted to those individuals having a defined need to know for the proper performance of their official duties.

3. The information may be disseminated outside the Department of Defense only as follows:

a. When required for the purposes described in Section 2517 of 18 U.S.C. (reference (a)).

b. When required by law, including the Privacy Act of 1974, as implemented in DoD Directive 5400.11 and the Freedom of Information Act of 1966, as implemented in DoD Directive 5400.7 (references (f) through (i)), or by order of a Federal court.

c. When requested by a Committee of the Congress.

d. When required by a SOFA or another international agreement.

D. RETENTION AND DISPOSITION OF RECORDS

The records of a wire, electronic, or oral communication interception not otherwise contained in the permanent criminal investigative case file shall be retained and disposed of in accordance with the records retirement procedures of the DoD Component. Recordings of interceptions made in the United States under Section 2518 of 18 U.S.C. (reference (a)) may be destroyed only under order of the court involved, and must be maintained at least 10 years.

E REPORTING REQUIREMENTS

1. To comply with the requirements of Appendix A and Section 2519 of 18 U.S.C. (reference (a)), the Secretaries of the Military Departments, or designees; the Director, DCIS, or designee; and the DPS, shall submit reports described in paragraphs E.1.a. through E.1.c. of this Chapter, below, to the Assistant Inspector General for Criminal Investigative Policy and Oversight, Office of Inspector General, Department of Defense, 400 Army Navy Drive, Arlington, VA 22202.

a. Annually. By October 31, an inventory of all devices that are primarily useful for interception of wire, electronic, and oral communications. The report has been assigned RCS DD-IG(A)1901. A suggested format is illustrated at Figure 2-1.

b. Annually. By December 31, a report of all nonconsensual interceptions of wire, electronic, and oral communications during the calendar year, and all unsuccessful applications for orders to do such interceptions during the calendar year. The report shall contain the information in Chapter 3, below. It has been assigned RCS DD-IG(A)1907.

c. Quarterly. For the quarters ending in March, June, September, and December, to be received by the 30th day of each following month, a report of all consensual interceptions of wire, electronic, and oral communications approved or done, or for which approval extensions were granted during the quarter. (In joint cases when another Federal Agency has requested and approved the consensual interception, duplicate reporting by the DCIO or the DPS is not required.) The report should follow the guidelines in Chapter 3. It has been assigned RCS DD-IG(Q)795.

2. Nonconsensual intercepts conducted in accordance with paragraph B.2.a. of Chapter 1 and all consensual intercepts conducted outside the United States are exempt from the reporting requirements of subsection E.1. of this Chapter, above.

3. The IG, DoD, shall consolidate all reports provided under subsection E.1., above, and provide them to the Attorney General of the United States.

ANNUAL INVENTORY FOR YEAR ENDING 30 JUNE (YYYY)

IDENTIFICATION OF REPORTING COMPONENT: _____

PART ONE: APPARATUS AND DEVICES ON HAND AT END OF YEAR

Description (Purpose)	Government Nomenclature	Mfgr.'s Nomenclature	Federal Stock #	Mfgr.'s Stock #	No. on Hand	Location of Devices (show amts. in each area) (Applies to Part I only)			
						U.S.	Europe	Pacific	Other

FOR OFFICIAL USE ONLY

CHAPTER 3

INFORMATION TO BE INCLUDED IN REPORTS OF INTERCEPTIONS OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS

A. CONSENSUAL INTERCEPTIONS

1. Identity of the DoD Component making the report

2. Number of total requests for authorization, broken down by offense or reason for the interception.

3. Number of emergency authorizations.

4. Number of times that the interceptions provided information that corroborated or assisted in corroborating the allegation or suspicion.

5. Number of authorizations not used.

B. NONCONSENSUAL INTERCEPTIONS

1. Identify the applying organization unit. Indicate whether the application was for a DoD Component other than the DoD Component making the report, or for a non-DoD activity. Identify the type of order or extension for which application was made.

2. A statement indicating whether the order or extension was modified or denied.

3. The period of interception authorized by the order, and the number and duration of any extensions of the order.

4. The offense specified in the order or application, or extension of an order.

5. The identity of the applying investigative or law enforcement officer and Agency making the application, and the person authorizing the application.

6. The nature of the facilities from which, or the place where, communications were to be intercepted.

7. A general description of the interceptions made under such order or extension, including:

a. The approximate nature and frequency of incriminating communications intercepted.

b. The approximate nature and frequency of other communications intercepted.

c. The approximate number of people whose communications were intercepted.

d. The approximate nature, amount, and cost of the manpower and other resources used in the interceptions.

8. The number of arrests resulting from interceptions made under the order or extension, and the offenses for which arrests were made.

9. The number of trials resulting from the interceptions

10. The number of motions to suppress made concerning such interceptions, and the number granted or denied.

11. The number of convictions resulting from the interceptions, the offenses for which convictions were obtained, and a general assessment of the importance of the interceptions.

12. The information required by subsections B.7. through B.11., above, for orders or extensions obtained in a preceding calendar year.

C. UNSUCCESSFUL APPLICATIONS FOR NONCONSENSUAL INTERCEPTION AUTHORIZATION ORDERS

1. Investigative case number or identifier for the application.

2. All information required in subsections B.1., B.2., and B.4. through B.6. of this Chapter, above.

3. Identity of the judge who denied the application and date of denial.

4. If the application was for an extension, indicate the dates, duration, and results of the previous interception.

5. Reason why the application was denied by the court (or, when judicial approval is not required, provide the reason why the application was denied by the approval authority). Do not include those disapproved at some level of review in the chain before actual presentation to an official empowered to authorize the nonconsensual interception.

CHAPTER 4

ELECTRONIC INTERCEPTION EQUIPMENT

A. CONTROL OF INTERCEPTION EQUIPMENT

1. The Military Departments; the DPS; and the IG, DoD, shall establish controls to ensure that only the minimum quantity of interception equipment required to accomplish assigned missions is procured and retained in inventories.

2. Interception equipment shall be safeguarded to prevent unauthorized access or use, with inventory records accounting for all equipment at all times. When equipment is withdrawn from storage, a record shall be made as to the times of withdrawal and its return to storage. Equipment shall be returned to storage when not in actual use, except when returning the equipment would interfere with its proper utilization. The individual to whom the equipment is assigned shall account fully, in a written report, for the use made of the equipment while it was removed from storage. Each Agency shall retain the completed inventories of equipment, the times of withdrawal and return, and the written reports of the agents specifying the uses made of the equipment, in accordance with its normal criminal investigative records retention policy, but not less than 3 years.

B. DISPOSAL OF INTERCEPTION EQUIPMENT

1. Federal law prohibits the manufacture, assembly, possession, or sale of any device by any person who knows, or has reason to know, that "...the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce" (Subsection 2512(1)(b) of 18 U.S.C. (reference (a+). Disposal outside the Government of interception equipment is prohibited.

a. Transfer of such interception equipment to law enforcement officials of State Governments is permitted if the transfer or subsequent possession does not violate any applicable State or local laws.

b. The Agency disposing of interception equipment must ensure that the equipment is transferred to an Agency authorized to use it or the equipment is destroyed.

2. If there are questions about the primary purpose of an item of equipment, the official involved shall prohibit its sale pending referral to the Secretary of the Military Department; the

IG, DoD; or the GC, DoD. The respective General Counsels shall resolve any legal issues in coordination with the GC, DoD.

Office of the Attorney General
Washington, D. C. 20530

November 7, 1983

MEMORANDUM TO: Heads and Inspectors General of
Executive Departments and Agencies

FROM: William French Smith
Attorney General

By the attached Memorandum, which addresses the investigatory use of devices to intercept and record certain consensual verbal communications, I am superseding Attorney General Civiletti's Memorandum of September 22, 1980, concerning "Procedures for Lawful, Warrantless Interceptions of Verbal Communication". The principal purpose of this action is to limit the instances in which agencies must follow the current procedure of obtaining advance written authorization from the Director of the Criminal Division's Office of Enforcement Operations to seven specified "sensitive" situations. (See Part II. A)

In all other cases, approval of a consensual surveillance will be at the agency level. (See Part V.) This provision requires that: (1) verbal authorization must be obtained from an appropriate Department of Justice attorney (i.e., normally one in the district where the interception is to occur); (2) all information which was previously submitted to the Department of Justice (see Part III. A 1-8) must now be submitted to the authorizing agency official; and (3) the authorizing agency official must be the agency head or a designated high-ranking supervisory official at headquarters level.

I am convinced that this change will improve the efficiency of consensual surveillances as an investigative tool without diminishing the protection afforded civil liberties. As the government's chief law enforcement officer, I ask you to assure close compliance with the procedures and rules of the attached Memorandum throughout your office, agency or department.

Office of the Attorney General
Washington, D. C. 20530

November 7, 1983

MEMORANDUM TO THE HEADS AND INSPECTORS GENERAL
OF EXECUTIVE DEPARTMENTS AND AGENCIES

Re: Procedures for Lawful, Warrantless Interceptions of Verbal Communications

By Memorandum dated October 16, 1972, the Attorney General directed all federal departments and agencies to obtain Department of Justice authorization before intercepting verbal communications without the consent of all parties to the communication. This directive was clarified and continued in force by the Attorney General's subsequent Memorandum of September 22, 1980, to Heads and Inspectors General of Executive Departments and Agencies.

This Memorandum supersedes the aforementioned directives. It establishes new authorization procedures with relevant rules and guidelines while it continues existing reporting procedures. It limits the requirement for prior written approval by the Department of Justice to specific types of investigations, but it continues to require verbal authorization from Department of Justice attorneys in all other types of investigations. This change in policy, eliminating prior written Department of Justice approval in most cases of consensual surveillance, is a result of the exercise of the Department's review function for some ten years. This experience reflects the fact that the departments and agencies have been uniformly applying the required procedures with great care, consistency, and good judgment, and that the number of inappropriate requests for consensual interceptions has been negligible.

The Fourth Amendment to the Constitution, Title III. of the Omnibus Crime Control and Safe Streets Act of 1968 as amended (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 and verbal, non-wire communications. United States v. White, 401 U.S. 745 (1971); United States v. Caceres, 440 U.S. 741 (1979). Similarly, the Constitution and

federal statutes permit federal agents to engage in warrantless interceptions of verbal, non-wire communications when the communicating parties have no justifiable expectation of privacy. 1/ 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 informants or undercover law enforcement agents, or fulfilling some other similarly compelling need. While these techniques are lawful and helpful, their use in investigations is frequently sensitive, so they must remain the subject of careful, self-regulation by the agencies employing them.

The sources of authority for this Memorandum are Executive Order No. 11396 ("Providing for the Coordination by the Attorney General of Federal Law Enforcement and Crime Prevention Programs"); Presidential Memorandum ("Federal Law Enforcement Coordination, Policy and Priorities") of September 11, 1979; Presidential Memorandum (untitled) of June 30, 1965, on, inter alia, the utilization of mechanical or electronic devices to overhear non-telephone conversations; and the inherent authority of the Attorney General as the chief law enforcement officer of the United States.

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.

1/ As a general rule, nonconsensual interceptions of verbal wire communications violate 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. of the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. §2510, et seq.) or with the provisions of the Foreign Intelligence Act of 1978 (50 U.S.C. §1801, et seq.).

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:

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;

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;

the interception relates to an investigation of a federal law enforcement official;

the consenting or nonconsenting person is a member of the diplomatic corps of a foreign country;

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;

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

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 in this Memorandum do not apply to:

extraterritorial interceptions;

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 III. of the Omnibus Crime Control and Safe Streets Act of 1968 as amended (18 U.S.C. §2510, et seq.);

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

interceptions of radio communications; and

interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information

The following information must be set forth on any request to intercept a verbal communication without the consent of all parties to the communication:

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

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

Danger. If an interception is for protection purposes, the request must explain the danger to the consenting party.

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.

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.

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.

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.

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 renewal 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. of this Memorandum 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 2/ must be conducted under tightly controlled circumstances. 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 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 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 investi-

2/ 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).

gation. 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.

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 electronic surveillance or any other form of nonconsensual interception.

11/7/83
DATE

ATTORNEY GENERAL