

# GENERAL ORDER



DISTRICT OF COLUMBIA

Title		
<b>Interception of Wire or Oral Communications</b>		
Topic	Series	Number
<b>SPT</b>	<b>304</b>	<b>04</b>
Effective Date		
<b>July 12, 2011</b>		
Replaces:		
General Order 304.4 (Interception or Recording of Wire or Oral Communications), Effective Date June 11, 2003		

I.	Background	Page 1
II.	Policy	Page 1
III.	Definitions	Page 2
IV.	Regulations	Page 2
V.	Procedures	Page 3
V.A.	Requesting Court Authorization	Page 3
V.B.	Interceptions or Recordings Not Requiring Court Authorization	Page 3
V.C.	Emergency One-Party Situations	Page 5
V.D.	After-Action Report	Page 5
V.E.	Issuance of Electronic Surveillance Equipment and Request for Services	Page 6
V.F.	Maintaining Department Owned Surveillance and Recording Equipment	Page 7
V.G.	Registration and Use of Privately Owned Surveillance and Recording Equipment	Page 8
V.I.	Roles and Responsibilities	Page 8
VII.	Cross References	Page 9

## I. BACKGROUND

There are four (4) acts of Congress which affect the interception/recording of communications; Title III of the Omnibus Crime Control and Safe Streets Act of 1968, the Electronic Communications Privacy Act of 1986, the Communications Assistance for Law Enforcement Act of 1994, and the Anti Terrorism Act of 1996. These Acts define, authorize and regulate the interception or recording of communications.

The contents of this general order complies with federal law and the provisions governing the interception of wire or oral communications, as established in D.C. Official Code §§23-541 thru 556 (Wire Interception and Interception of Oral Communications).

## II. POLICY

It is the policy of the Metropolitan Police Department (MPD) to adhere to the laws, rules and regulations governing the interception of wire or oral communications in a manner that does not violate an individual's constitutional rights.

### III. DEFINITIONS

When used in this directive, the following terms shall have the meanings designated:

1. Electronic Communications – The transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo optical system (e.g., fax, pager, cellular telephone or e-mail).
2. Intercept – The aural acquisition of the contents of any wire or oral communication through the use of any intercepting device.
3. Intercepting Device – Any electronic, mechanical, or other device or apparatus that can be used to intercept a wire or oral communication other than:
  - a. Any telephone, equipment, or facility, or any component thereof, furnished to the MPD by a communications common carrier in the ordinary course of its business and being used by an investigative or law enforcement officer in the ordinary course of his/her duties.
  - b. A hearing aid or similar device being used to correct subnormal hearing.
4. One-Party Consent – Interception of wire and oral communications by the MPD, without having to obtain court authorization (e.g., when there is the consent of a party whose voice is being intercepted).
5. Oral Communications – Any oral communications uttered by a person exhibiting an expectation that the communication is not subject to interception under circumstances justifying the expectation.
6. Surveillance and Recording Equipment – Any telephone extension, device or bug, whether mechanical, electrical, battery operated, wire or wireless, that will intercept, eavesdrop, monitor, pick-up or record any oral conversation, except that tape recorders are explicitly exempted.
7. Wire Communications – Any communication 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, furnished or operated by any person engaged as a common carrier in providing or operating such facilities.

### IV. REGULATIONS

- A. Members making a request to conduct interceptions of wire or oral communications, which is not one-party consent, must obtain court authorization.

- B. Requests to utilize electronic surveillance equipment shall be submitted and hand carried to the Commander, Narcotics and Special Investigations Division (NSID), Investigative Services Bureau, on a PD Form 154 (Request for Services of Electronic Surveillance Unit).
- C. **Due to the extremely sensitive and confidential nature of investigations conducted by the Internal Affairs Bureau (IAB), the Assistant Chief, IAB, shall be authorized to obtain, maintain, and utilize electronic surveillance equipment for investigations conducted by IAB members in accordance with the procedures enumerated in this directive. Any requests dealing with interception of wire or oral communications by members of IAB shall be submitted to the Assistant Chief, IAB.**

## V. PROCEDURES

- A. Requesting Court Authorization
  - 1. Members shall submit all requests for court authorization to conduct interceptions of wire or oral communications through channels, to the Assistant Chief, Investigative Services Bureau.
  - 2. Members shall hand carry all requests to the Assistant Chief, Investigative Services Bureau or his/her designee, for approval.
  - 3. With approval of the Assistant Chief, Investigative Services Bureau, members shall submit requests to an Assistant United States Attorney, who may authorize, in writing, a member to make application to the court for an order authorizing the interception of oral or wire communications.
  - 4. Upon completion of all court approved wire or oral interceptions, members shall submit a report detailing the results obtained from the interception to the Assistant Chief, Investigative Services Bureau.
- B. Interceptions or Recordings Not Requiring Court Authorization
  - 1. One-party consent conversations that take place within the District of Columbia may be intercepted, monitored, or recorded by the MPD, without having to obtain court authorization.
  - 2. Members **shall not** submit one-party consent requests electronically through the Adminbox or through departmental mail.
  - 3. Routine One-Party Consent Request

- a. When time is not a critical factor, the member shall obtain prior written authorization from the Assistant Chief, Investigative Services Bureau before any member intercepts; records; or listens in on any conversation, utilizing any electronic surveillance equipment or any other aid to the human hearing, without the clearly expressed or implied consent of **all** parties to such conversation.
  - b. Reasonable one-party consent requests will be approved for no longer than sixty (60) days. At the expiration of the sixty (60) day period, the member will not longer have authorization to intercept communications and must apply for an extension.
4. Members shall ensure one-party consent requests contain the following:
- a. Enough information to identify the specific investigation involved. If the investigation is confidential, a control number for the type of investigation being conducted (e.g., gambling, narcotics) is sufficient.
  - b. The type of interception or recording (e.g., oral or telephonic) to be made.
  - c. The date(s) the interception or recording is to take place.
  - d. The name of the person(s) consenting to have the conversation recorded or intercepted. In the case of undercover officers or special employees, his/her identifying number shall be given.
  - e. The jurisdiction in which the recording or interception is to take place.
    - (1) If the request is for a one-party consent recording or interception in the state of Maryland, the name of the person or agency in that jurisdiction, under whose direction the requesting member shall conduct the operation shall be specified.
    - (2) In the state of Maryland, only Maryland state investigative or law enforcement officers, or any other person acting at the direction or under the direct supervision of a Maryland investigative or law enforcement officer, or any attorney authorized to prosecute or assist in the prosecution of criminal cases in the state of Maryland, are authorized to conduct one-party consent recordings.

Authorization can only be given for the investigation of murder, kidnapping, gambling, robbery, bribery, extortion, dealing in controlled dangerous substances, or the conspiracy to commit any of these seven (7) offenses.

- (3) In the state of Virginia, there are no restrictions concerning the conduct of one-party consent activities. However, members planning to operate in Virginia shall, if time permits, contact the Virginia prosecuting Attorney's office to make sure the activity, which is being conducted, meets with their approval. If time is a factor, adhere to the procedures in Part V.C. of this order.

#### C. Emergency One-Party Consent Situations

In situations when the progress of an investigation makes it necessary to use surveillance or recording equipment immediately to intercept communication with the consent of one-party, the requesting member shall:

1. Make an oral request to the Assistant Chief, Investigative Services Bureau, or designee;
2. Obtain an Investigative Services Bureau control number; and
3. Prepare a written request (described above) on the next business day that indicates the date and time the oral request was granted.

#### D. After-Action Report

1. Upon concluding a one-party consent operation, authorized as a result of a written request, the member who requested the consent shall:
  - a. Prepare a report indicating whether or not the interception or recording was made.
  - b. Provide any information that differs from the original request.
  - c. Prepare and submit the report, with the Investigative Services Bureau control number on the report, to the Assistant Chief, Investigative Services Bureau.
2. In emergency cases, the member who requested the consent shall:
  - a. Prepare a report containing the information prescribed in a regular one-party consent requests. The member shall:

- (1) Ensure the report contains a statement as to whether or not the interception or recording was made.
      - (2) Include the reason the one-party consent request was considered an emergency.
      - (3) Include the Investigative Services Bureau control number.
    - b. Submit the report to the Assistant Chief, Investigative Services Bureau, by 0900 hours on the next business day.
  3. Extension of one-party consent requests
    - a. Members shall ensure that all one-party consent requests for extensions are submitted within sixty (60) calendar days of the date that the initial request is approved.
    - b. If a member submits an extension request for approval past the sixtieth (60<sup>th</sup>) day, it shall be disapproved, and the member shall complete an after action report prior to the approval of a new request.
- E. Issuance of Electronic Surveillance Equipment and Request for Services
1. Members of an organizational element that requires surveillance equipment on a continuous basis may arrange for the automatic issuance of equipment, through the Commanding Officer, NSID, or his/her designee. The member of the organizational element shall establish a schedule with the, NSID, Electronic Surveillance Unit for inspections of the equipment every ninety (90) days.
  2. Unless specific authorization has been granted by an official of the Electronic Surveillance Unit, members shall ensure all issued equipment is returned prior to the expiration of their shift in which the equipment was issued.
  3. An official of the Electronic Surveillance Unit may grant an extension beyond the expiration of the shift.
  4. Extensions beyond thirty (30) days shall be granted, only upon the submission of written justification, from the element's commanding officer and approval by the Commanding Officer, NSID.

F. Maintaining Department Owned Surveillance and Recording Equipment

1. Members of the Electronic Surveillance Unit shall ensure all surveillance and recording equipment that is the property of the Metropolitan Police Department is registered in accordance with Part V.F.2 of this order.
2. Electronic Surveillance Units members shall:
  - a. Store and establish an inventory database to catalogue the surveillance and recording equipment. The database must contain, at a minimum, the following information:
    - (1) Brand name and type of surveillance or recording equipment;
    - (2) Serial and model number;
    - (3) Date of purchase or acquisition;
    - (4) District or unit where equipment is assigned; and
    - (5) Name of member responsible for maintenance and distribution of equipment.
  - b. Conduct quarterly, documented, inspections of electronic surveillance equipment, for the purpose of maintaining operational readiness, which includes:
    - (1) Detecting any wear;
    - (2) Abuse;
    - (3) Neglect; and
    - (4) Taking necessary action to correct or repair equipment.
  - c. Maintain records of maintenance to include any repair costs.
  - d. Evaluate and issue the inventory of electronic surveillance equipment.
  - e. Place all orders, through the chain of command to the Director, Equipment and Supplies Branch, General Support Services Division, Corporate Support Bureau, for all expendable supplies required to support electronic surveillance equipment.

G. Registration and Use of Privately Owned Surveillance and Recording Equipment

1. No privately owned surveillance or recording equipment, (other than tape recorders) may be brought into, kept or used on MPD premises or in connection with MPD business or investigations, unless it has been registered on a PD Form 298 (Registration of Surveillance and Recording Equipment) with an administrative official of the relevant organizational unit (e.g., Electronic Surveillance Unit or IAB).
2. Privately owned surveillance and recording equipment, which is only temporarily brought into or left at a MPD facility, for a period of time not to exceed a member's shift, and which is in transit for private purposes, is not subject to registration.
3. Privately owned surveillance and recording equipment shall only be used in connection with MPD business or investigations, by its registered owner, in accordance with this directive or with the explicit approval of the official in command of the relevant organizational unit. The approving official shall ensure that any use is consistent with the guidelines set forth in this order.

**VI. ROLES AND RESPONSIBILITIES**

A. Officials shall ensure that:

1. Use of surveillance or recording equipment by members of their respective element is conducted in accordance with the provisions of this order.
2. NSID electronic surveillance equipment assigned to their unit is maintained securely when not in use and is inspected prior to and after use.

B. Commanding Officers shall ensure that:

1. All electronic surveillance equipment not assigned to the IAB is properly registered with the Electronic Surveillance Unit.
2. A member of their command is assigned the responsibility for the distribution and maintenance of surveillance equipment.

C. The Assistant Chief of Police, Investigative Services Bureau, shall:

1. Submit to the Chief of Police, by the fifteenth (15<sup>th</sup>) calendar day of

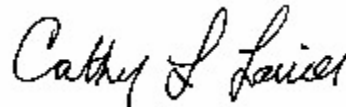


January, a report of all recording and surveillance activities for the previous calendar year that did not require court authorization, but were authorized under the provisions of this order.

2. Ensure that the Electronic Surveillance Unit conducts an annual inventory of all MPD-owned surveillance and recording equipment.
3. Ensure that the Electronic Surveillance Unit conducts an annual review of all registered, privately-owned surveillance and recording equipment.

## VII. CROSS REFERENCES

- A. D.C. Official Code §§23-541 thru 556 (Wire Interception and Interception of Oral Communications)
- B. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (U.S.C. §§ 2510)
- C. Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, 100 Stat.1848)
- D. Communications Assistance for Law Enforcement Act of 1994 (Pub. L. No. 103-414, 108 Stat. 4279)
- E. Anti Terrorism Act of 1996 (Pub. L. No. 104-132, 110 Stat. 1214)



Cathy L. Lanier  
Chief of Police

CLL:PAB:MOC:CC:JC