Army Regulation 190–53

Military Police

# Interception of Wire and Oral Communications for Law Enforcement Purposes

Headquarters
Department of the Army
Washington, DC
16 July 2018

UNCLASSIFIED

# SUMMARY of CHANGE

AR 190–53
Interception of Wire and Oral Communications for Law Enforcement Purposes

This administrative revision, dated 20 September 2023—

- Changes proponency from the Provost Marshal General to the Director, U.S. Army Criminal Investigation Division (title page).

This major revision, dated 16 July 2018—

- Updates responsibilities (para 1–4).
- Updates the approval authorities concerning interception operations (para 1–4).
- Delegates approval authority for consensual interceptions (para 1–4).
- Specifies the only Department of Army law enforcement activity authorized to use technical listening equipment and conduct interceptions is the Criminal Investigation Division (para 1–6).
- Specifies that interception of oral communications of certain individuals requires Department of Justice written approval (para 3–5).
- Adds policy concerning the use of Global Positioning Systems trackers (para 4–6).
- Eliminates the requirement to submit annual reports to the Department of Defense (formerly para 7–1).
- Renumbers paragraphs (throughout).

**Headquarters**
**Department of the Army**
**Washington, DC**
**16 July 2018**

# *Army Regulation 190–53

**Effective 17 August 2018**

**Military Police**

# Interception of Wire and Oral Communications for Law Enforcement Purposes

By Order of the Secretary of the Army:

MARK A. MILLEY
*General, United States Army*
*Chief of Staff*

Official:

MARK F. AVERILL
*Acting Administrative Assistant*
*to the Secretary of the Army*

**History.** This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

**Summary.** This regulation implements DODI O–5505.09. It provides legal and technical policy for the U.S. Army Criminal Investigation Command law enforcement officials and legal officers. This regulation contains complex technical policies and procedures that may not be readily comprehensible to persons without extensive legal training and experience. Questions concerning policies contained herein should be discussed with supervisory personnel and legal advisors.

**Applicability.** This regulation applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated. This regulation also applies to all active duty and reserve special agents and investigative personnel assigned to the U.S. Army Criminal Investigation Command conducting investigations under the provisions of AR 195–2.

**Proponent and exception authority.** The proponent of this regulation is the Director, U.S. Army Criminal Investigation Division. Only the Secretary of the Army or designee may approve exceptions or waivers to this regulation that are consistent with controlling law and regulations. Activities may request a waiver to this regulation by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent and the approval authority. Refer to AR 25–30 for specific requirements.

**Army internal control process.** This regulation contains internal controls provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app B).

**Supplementation.** Supplementation of this regulation and establishment of command and local forms are prohibited without prior approval from the Director, U.S. Army Criminal Investigation Division.

**Suggested improvements.** Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.belvoir.hqda-usacid.mbx.cidpolicy@army.mil.

**Distribution.** This regulation is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

**Contents** (Listed by paragraph and page number)



*This regulation supersedes AR 190-53, dated 3 November 1986.



**UNCLASSIFIED**

## Chapter 1
## General

### 1–1. Purpose
This regulation provides Department of the Army (DA) policies, procedures, and restrictions governing interception of wire and oral communications, use of pen registers and related devices, and the use of Global Positioning Systems (GPS) tracking systems for law enforcement purposes, both in the United States and abroad.

### 1–2. References
See appendix A.

### 1–3. Explanation of abbreviations and terms
See glossary.

### 1–4. Responsibilities
*a.* The Secretary of the Army—

(1) Is responsible for promulgation and oversight of DA policy for activities conducted under this regulation and DODI O–5505.09.

(2) Authorizes the Army General Counsel the authority to approve or deny requests for interception of wire, electronic, and oral communications for law enforcement purposes in accordance with this regulation and DODI O–5505.09.

(3) Will furnish to the Inspector General, DOD, Investigative Policy and Oversight, the list of designations made in accordance with DODI O–5505.09.

(4) Will ensure military judges are designated by The Judge Advocate General (TJAG) to administer the duties of authorizing nonconsensual interceptions of wire, electronic, and oral communications for CID personnel when the target is subject to the Uniformed Code of Military Justice (UCMJ) and the operation/investigation is being conducted outside the United States and its territories.

*b.* The Army General Counsel will —

(1) Ensure compliance with the policies and procedures set forth in this regulation and referenced in DODI O–5505.09.

(2) Approve or deny requests to seek judicial authorization for nonconsensual interception of wire, electronic, oral communications, and pen register operations received from CID field elements. A copy of all approved concepts for nonconsensual interception will be retained by the Office of the Army General Counsel.

(3) Approve or deny requests to conduct one party consensual interceptions of wire, electronic, and oral communications and pen register operations. The General Counsel is the designated approval authority of these requests and has the authority to designate additional approval authorities consistent with DODI O–5505.09. A copy of all approved concepts for nonconsensual interception will be retained by the Office of the Army General Counsel.

*c.* TJAG will assign military judges, certified in accordance with the provisions of the UCMJ Art. 26, to receive applications to conduct nonconsensual interceptions of wire, electronic, and oral communications for CID personnel and to issue orders authorizing such operations in accordance with paragraph 3–2 of this regulation. The authority of such military judges to issue orders authorizing operations will be limited to instances when the target is subject to the UCMJ and the operation/investigation is being conducted outside the United States and its territories. Office of the Judge Advocate General will, in the case of interceptions governed by Title 18, United States Code, Chapter 119 (18 USC Chapter 119) for which a court order has been obtained, advise the CID official in charge of the operation on the requirements of 18 USC Chapter 119 and review the compliance with such requirements.

*d.* The Commander, CID will—

(1) Ensure compliance with the policies and procedures set forth in this regulation, and referenced in DODI O–5505.09. A copy of all approved consensual interception requests will be retained by HQ, CID.

(2) Validate any requests from CID field elements to the Army General Counsel for approval to seek judicial authorization for nonconsensual interception of wire, electronic, oral communications, and pen register operations.

(3) Issue regulations specifying storage and access requirements for applications, orders, recordings, and other records of information obtained through interception activities. The regulations include provisions for storage and access while the case is active and after the case has become inactive when the records have been transferred to a centralized facility.

(4) Develop regulations, policies, procedural controls, and designate responsible officials for both internal and external dissemination of the information. Procedures require creation and maintenance of records reflecting dissemination of that information.

(5) Ensure that the records and other information required in this regulation are established, and that DODI O–5505.09 is maintained.

(6) Ensure that controls are established for procurement and maintenance of interception equipment.

(7) Ensure that personnel involved in the activities and techniques discussed in this regulation are trained properly in applicable requirements and controls, including awareness of the criminal and civil sanctions for the illegal interception of wire, electronic, and oral communications.

*e.* All CID group commanders will ensure compliance with the policies and procedures set forth in this regulation and referenced in DODI O–5505.09.

### 1–5. Scope

*a.* The provisions of this regulation apply to all special agents and investigative personnel assigned to the U.S. Army Criminal Investigation Command. Army National Guard and U.S. Army Reserve special agents and investigative personnel are subject to the provisions of this regulation only following mobilization or call to active Federal service to conduct investigations under the provisions of AR 195–2.

*b.* This regulation does not affect Status of Forces Agreements (SOFAs) or other specific agreements that may otherwise limit implementation of provisions in any particular geographical area abroad.

*c.* This regulation is not applicable to—

(1) U.S. Army intelligence activities (see AR 381–10).

(2) Administrative telephone monitoring and recording activities and command management monitoring activities (see AR 25–1).

(3) DA communication security activities (see AR 380–53).

(4) Monitoring telephone communications in DA Command and Control System Operations Centers (see AR 25–1).

(5) Interceptions arising from technical surveillance countermeasures surveys (see AR 381–14).

(6) Interceptions for foreign intelligence and counterintelligence purposes, except when the interception occurs during an investigation of criminal acts of espionage, sabotage, or treason conducted under the provisions of AR 381–20.

(7) Recording of emergency telephone and/or radio communications at Military Police Operations desks (see AR 190–30).

(8) Closed circuit recording systems, to include those with an audio capability, employed for security purposes (see AR 190–30).

(9) The recording of interviews and interrogations by law enforcement personnel.

(10) Interceptions arising from overt video or audio equipment installed in DOD traffic or law enforcement patrol vehicles or worn by uniformed law enforcement officers.

### 1–6. General

*a.* The electronic, mechanical, or other device recording of wire and oral communications for law enforcement purposes is prohibited unless conducted in accordance with this regulation, DODI O–5505.09, and applicable law.

*b.* The only DA element authorized to intercept wire and oral communications and conduct pen register operations under this regulation are the CID investigative personnel for investigations conducted under the provisions of AR 195–2.

*c.* Nonconsensual interception of wire and oral communications is a special technique which will not be considered as a substitute for normal investigative procedures and will be authorized only in those circumstances where it is demonstrated that the information is necessary for a criminal investigation and cannot reasonably be obtained in another, less intrusive manner.

*d.* Nonconsensual interception of wire and oral communications is prohibited unless there exists probable cause to believe that—

(1) In the case of interceptions within the United States, a criminal offense listed in 18 USC 2516 has been, is being, or is about to be committed.

(2) In the case of interceptions abroad conducted pursuant to an order issued by a military judge under paragraph 2–2*a* of this regulation, one of the following violations of the UCMJ has been, is being, or is about to be committed by a person subject to the UCMJ.

*(a)* The offense of murder, manslaughter, kidnapping, gambling, robbery, sexual assault, bribery, extortion, espionage, sabotage, treason, fraud against the government, or dealing in narcotic drugs, marihuana, or other dangerous drugs.

*(b)* Any other offense dangerous to life, limb, or property, and punishable by death or confinement for 1 year or more.

*(c)* Any conspiracy to commit any of the foregoing offenses listed in paragraphs 1–6*d*(2)(*a*) and 1–6*d*(2)(*b*).

(3) In the case of other interceptions abroad, conduct which would constitute one of the offenses listed in 18 USC 2516(1) and 2516(2) if committed in the United States, has been, is being, or is about to be committed to include any conspiracy to commit any of the forgoing offenses.

*e.* Consensual interceptions of wire and oral communications will be undertaken only when at least one of the parties to the conversation has consented to the interception and when the investigation involves:

(1) A criminal offense punishable under the USC, UCMJ, or state criminal code by death or confinement for 1 year or more.

(2) A telephone call involving obscenity, harassment, extortion, bribery, bomb threat, or threat of bodily harm that has been made to a person authorized to use the telephone of a subscriber-user on an installation, building, or portion thereof, under DOD jurisdiction or control, and when the subscriber-user has also consented to the interception.

*f.* The prohibitions and restrictions of this regulation apply regardless of the official use or dissemination of the intercepted information. Any questions as to whether the use of a particular device may involve prohibited wire or oral interception will be submitted with supporting facts through command channels to the Army General Counsel for resolution.

*g.* No otherwise privileged wire or oral communication intercepted in accordance with this regulation will lose its privileged character.

*h.* CID personnel are authorized to monitor telephone conversations (including cellular phone, voice over internet protocol, and so on) by use of an extension telephone instrument, and text message communication, instant messages, and so on, with the consent of at least one party to the conversation, provided the monitoring is done solely for a valid law enforcement purpose and is not recorded.

## Chapter 2
## Procedures Governing Consensual Interceptions of Wire and Oral Communications

### 2–1. Consensual interceptions of communications

*a.* The following procedures are applicable to all one party consensual interceptions of oral or wire communications:

(1) The CID special agent must request written approval from the approval authority before engaging in a consensual interception of oral communication. This includes any recordings of phone conversations and utilization of a cellular phone as a technical listening device.

(2) The CID special agent prepares a written request including at least the following information:

*(a) Reasons for the interception.* A reasonably detailed statement of the background of the investigation and the need for the interception.

*(b) Offense.* If the interception is for investigative purposes, a citation of the criminal statute involved.

*(c) Danger*. If the interception is intended to provide protection to the consenting party, explain the nature of the danger to the consenting party.

*(d) Location and type of device.* A general description of the type of device to be used, along with a description of where the device will be hidden—on the person, in personal effects, or in a fixed location.

*(e) Location of interception.* The physical location and primary federal jurisdiction where the interception will take place. If the location changes, the criminal investigator promptly provides written notice to the approving official.

*(f) Time.* The length of time needed to conduct the interception and get the necessary information. An authorization may be granted for up to 90 days from the day the interception is scheduled to begin. Authorization to intercept may be renewed for 90 days upon reapplication.

*(g) Names.* The names of persons, if known, whose communications are expected to be intercepted and their relation to the matter under investigation or the need for the interception. Identify whether the persons are consenting or nonconsenting parties to the intercept. If the consent is not obtained in writing, submit a statement on how consent was obtained. Names of undercover operatives, cooperating citizens, or informants may be identified by an individualized informant or source number.

*(h) Attorney advice.* An attestation from the appropriate attorney regarding the legal sufficiency of the request is required. More information about this requirement can be found in policy regarding this review.

(3) A request to renew authority to intercept contains all the information required for the initial request. It is submitted to the approval authority for approval. The renewal request must also refer to all previous authorizations, explain why additional authorization is needed, and provide updated attorney endorsement on the renewal request.

(4) Excluding any exceptions noted elsewhere in this regulation (for example, emergency situations and joint investigations), consensual interceptions of wire, electronic, and oral communications will be authorized in writing by the approval authority or designee, after a legal sufficiency review. The approval authority will maintain the approval or denial in a filing system.

*b.* CID special agents may employ consensual interception techniques without approval based on approvals granted to or obtained by another federal, state, or local law enforcement agency, with which CID is engaged in a joint investigation. However, notifications will be submitted to HQ, CID, when any of the following occur:

(1) DOD personnel participate in the monitoring.

(2) Defense Criminal Investigative Organization equipment is used in the monitoring.

(3) The monitoring takes place on a DOD installation.

### 2–2. Emergency request for consensual interception

*a.* When an emergency situation exists or evidence of significant criminal conduct is likely to be lost before the written application can be processed, the CID special agent may seek verbal authorization for one party consensual interception from the approving official after consulting with the AUSA, SAUSA, supporting JA, or legal counsel associated with the particular investigation.

*b.* Within 48 hours, the CID field element will follow up with a written request to the approving official containing all the information required under paragraph 2–1 of this regulation.

### 2–3. Consensual monitoring

*a.* With the consent of one of the parties to a telephone conversation, CID personnel are authorized to monitor telephone conversations (including cellular phone, voice over internet protocol, and so on), by use of an extension telephone instrument, provided the monitoring is done solely for a valid law enforcement purpose. By the fact that such monitoring occurred, a summary of the conversation will be included in the law enforcement report. Only those parts of the conversation dealing with the law enforcement purpose will be contained in the summary. Such monitoring is not considered an interception of wire or oral communication; however, any recordings of conversations under these circumstances must comply with paragraph 2–1 of this regulation. Only CID investigative personnel are authorized to conduct the consensual interception.

*b.* Army law enforcement personnel are authorized to monitor text message communication, instant messages, and so on, with the consent of at least one party to the conversation, provided the monitoring is done solely for a valid law enforcement purpose. Such monitoring is not considered an interception of wire or oral communication. Taking photographs of the texts, internet chat, and so on, or conducting forensic extractions of the digital evidence does not constitute an intercept and requires no prior approval in accordance with this regulation. By the fact that such monitoring occurred, a summary of the conversation will be included in the law enforcement report. Only those parts of the conversation dealing with the law enforcement purpose will be contained in the summary.

## Chapter 3
## Procedures Governing Nonconsensual Interceptions of Wire and Oral Communications and Interceptions Requiring Special Approval

### 3–1. Nonconsensual interception in the United States

When an interception is deemed necessary for a criminal investigation, the following procedures are applicable:

*a.* The requesting CID element will prepare and forward a "request for authorization" to the group HQ for review and approval to seek judicial authorization. Each request for authorization will contain the following information:

(1) The identity of the CID special agent official making the application.

(2) A complete description of the facts and circumstances relied upon by the applicant to justify the intended interception, including—

*(a)* The particular offense that CID has probable cause to believe has been, is being, or is about to be committed.

*(b)* A description of the type of communication sought to be intercepted with a statement of the relevance of that communication to the investigation.

*(c)* A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted.

*(d)* The identity of the person, if known, committing the offense and whose communications are to be intercepted.

(3) A statement as to whether other investigative procedures have been tried and failed or why other procedures reasonably appear to be unlikely to succeed if tried or are too dangerous.

(4) An identification of the type of equipment to be used to make the interception.

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

(6) The procedures to minimize the acquisition, retention, and dissemination of information unrelated to the purpose of the interception.

(7) A complete statement of the facts concerning each previous application for approval of interceptions of wire or oral communications known to the applicant and involving any of the same persons, facilities, or places specified in the application and the action taken thereon.

(8) When the application is for an extension of an order, a statement setting forth the results thus far obtained from the interception, or an explanation of the failure to obtain such results.

(9) If this request is leaving the Department of the Army, there must be a written endorsement from the servicing SJA's office of the appropriate GCMCA.

*b.* Upon receipt of the request, the group JA will review the request to ensure compliance with the requirements of this regulation, DODI O–5505.09, 18 USC Chapters 119 and 206, and any other applicable law or policy.

*c.* Approval or disapproval of all Requests for Authorization will be made in writing by the group commander and retained as required by this regulation.

*d.* If the request is approved by the group commander, the official making the request or a designated representative will coordinate directly with the U.S. Attorney's Office for preparation of documents necessary to obtain a court order in accordance with 18 USC 2518. These documents will be forwarded by the DOJ attorney to the Attorney General, or to the designated Assistant Attorney General, for approval in accordance with 18 USC 2516. Initial contact with the attorney from DOJ or from the U.S. Attorney's office may be made while the request is being processed.

*e.* Upon approval by the Attorney General, or the designated Assistant Attorney General, formal application for a court order will be made by the appropriate attorney from the DOJ, assisted, if required, by an appropriate military lawyer.

*f.* Upon receipt of a court order and initiation of the interception operation in accordance with the term of the court order, the CID special agent in charge of the operation will consult with the U.S. Attorney's Office for advice on the requirements of 18 USC Chapter 119, and will provide such information to that office as is needed to demonstrate compliance.

*g.* If CID is not the lead investigative agency, CID is not responsible for obtaining approval or notification when the lead investigative agency obtains nonconsensual interception approval.

### 3–2. Nonconsensual interceptions abroad

Unless otherwise authorized by direction of the DOD, the following procedures are applicable to interceptions for law enforcement purposes when the interception takes place abroad and when an Army element, or members thereof, conduct or participate in the interception, or when the interception takes place abroad, is targeted against a U.S. person, and is conducted pursuant to a request by an Army element.

*a.* When the target of the interception is a person subject to the UCMJ—

(1) The request for authorization will include the information required by paragraph 3–1*a* of this regulation, and will be forwarded by the requesting CID field element in the same manner as for consensual interceptions in the United States. Approval or disapproval of all Requests for Authorization will be made in writing by the approving authority based on the standards set forth in paragraph 1–4 of this regulation and all applicable legal requirements.

(2) Upon written approval, the CID special agent or a designated representative will prepare a formal application for a court order in accordance with the procedure of 18 USC 2518(1). The application will be submitted to a military judge assigned to consider such applications pursuant to paragraph 1–4*c* of this regulation.

(3) Only military judges assigned by TJAG to receive applications for intercept authorization orders will have the authority to issue such orders. The authority of military judges to issue intercept authorization orders will be limited to interceptions conducted abroad and targeted against persons subject to the UCMJ.

*(a)* No military judge who has issued an order authorizing interceptions may act as the accuser, be a witness for the prosecution, or participate in any investigative or prosecutorial activities in the case for which an order was issued. A military judge who has issued an order authorizing interceptions is not qualified from presiding over the court-martial in the same case.

*(b)* A military judge otherwise qualified under paragraphs 3–2*a*(3)(*a*) and (b) of this regulation will not be disqualified from issuing orders authorizing interceptions because the judge is a member for a Service different from that of the target of the interception or from that of the investigative or law enforcement officers applying for the order.

(4) The military judge may enter an ex parte order, as requested or as modified, authorizing or approving an interception of wire or oral communications if the judge determines on the basis of the facts submitted by the applicant that—

*(a)* There is probable cause to believe that a person subject to the UCMJ is committing, has committed, or is about to commit a particular offense enumerated in paragraph 1–6*d* of this regulation.

*(b)* Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

*(c)* There is probable cause to believe that particular communications concerning that offense will be obtained through such interception.

*(d)* There is probable cause to believe that the facilities from which, or the place where, the wire or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

*(e)* The interception will not violate the relevant SOFA or the applicable domestic law of the host nation.

(5) Each order authorizing an interception will specify—

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

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

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

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

*(e)* The period of time during which such interception is authorized, including a statement as to whether the interception will terminate automatically when the described communication has been first obtained.

(6) Every order and extension thereof will contain a provision that the authorization to intercept will be executed as soon as practicable, will be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this regulation, and will be terminated upon attainment of the authorized objective.

(7) No order entered by a military judge may authorize an interception for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 60 days. Extensions of an order may be granted, but only upon application for an extension made in accordance with the procedures of 18 USC 2518(1), and after the military judge makes the findings required by paragraph 3–2*a*(4). The period of extension will be no longer than is necessary to achieve the purpose for which it was granted and in no event for longer than 60 days. Applications for extensions must be forwarded through channels in the same manner as prescribed for original applications.

(8) The contents of communications intercepted pursuant to an order issued by a military judge will, if possible, be recorded in a manner that will protect the recording from editing or other alterations. Custody of recording will be maintained in accordance with AR 195–5. Recordings will not be destroyed, except pursuant to paragraph 8–4, of this regulation.

(9) The contents of a communication intercepted abroad, or evidence derived therefrom, is inadmissible in any court-martial proceeding, in any proceeding under UCMJ Art. 15, or in any other proceeding if the—

*(a)* Communication was intercepted in violation of this regulation or applicable law.

*(b)* Order of authorization under which it was intercepted is insufficient on its face.

*(c)* Interception was not made in conformity with the order of authorization.

*b.* When the target of an interception is subject to federal prosecution under Military Extraterritorial Jurisdiction Act (MEJA)—

(1) The interception is permitted in accordance with U.S. laws.

(2) The interception does not violate host country laws, any applicable SOFA, or other agreements with host country authorities.

(3) The target's rights under the Fourth Amendment to the U.S. Constitution are not infringed.

(4) The procedures outlined above are followed.

*c.* When the target of an interception conducted abroad is a person who is not subject to the UCMJ, federal prosecution under the MEJA, or other possible prosecution in federal district courts, 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 CID field element will coordinate with local law enforcement agencies or prosecutor for the requirements to conduct the interception operation.

### 3–3. Emergency nonconsensual interceptions in the United States and abroad

*a.* When an emergency situation exists as described in 18 USC 2518(7) and there is not sufficient time to obtain an authorization, the Office of General Counsel may authorize the interception of wire, electronic, or oral communication or seek emergency approval from the Attorney General.

*b.* Within 48 hours after the interception occurs or begins to occur, the Office of Enforcement Operations (OEO), DOJ, must be notified. The OEO will seek authorization for the interception from the Attorney General.

### 3–4. Time limits for nonconsensual interceptions

Nonconsensual interceptions within the United States may be approved for a period not to exceed 30 days. Nonconsensual interceptions outside the United States may be approved for a period not to exceed 60 days. Renewal requests for specified periods of not more than 30 days each (60 days for interceptions outside the United States), will be submitted to the approving authority for consideration in the same manner as prescribed for original applications. In all instances, the interception will be terminated as soon as the desired information is obtained or when the interception proves to be nonproductive.

### 3–5. Interception of oral communication requiring written Department of Justice prior approval

Requests for written authorization from the OEO, DOJ to monitor an oral communication without the consent of all parties to the communication must contain the information described in paragraph 2–1 of this regulation. Requests will be sent to U.S. Department of Justice, Director, Office of Enforcement Operations, 950 Pennsylvania Avenue, NW, Washington, DC 20530–0001.

*a.* The Director or Associate Director, OEO, DOJ, must approve the request and must be notified when it is known that—

(1) The monitoring 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 monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any state or territory, or a judge or justice of the highest court of any state or territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties.

(3) Any party to the communication is a member of the diplomatic corps of a foreign country.

(4) Any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers.

(5) The consenting or nonconsenting person is in the custody of the Bureau of Prisons or the U.S. Marshals Service.

(6) The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the U.S. Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

(7) Written requests for authorization to intercept under any of these sensitive circumstances in paragraphs 3–5*a*(1) through (6) will be approved by the Commander, CID, or designee, then submitted by the Army General Counsel, or designee, to the OEO for review and processing.

*b.* Emergency authorization procedures are as follows:

(1) An emergency request for a consensual intercept, where written DOJ approval is required because of the sensitive circumstances, may be made by telephone to the DOJ approval officials listed in Section 9–7.302.III.B of the Attorney General Memorandum dated 30 May 2002 by a criminal investigator after a legal review and approval by the approval authority or designee.

*(a)* The criminal investigator puts the request in writing and submits it to the Commander, CID, or designee, as soon as practicable after authorization has been obtained. If the officials listed in Section 9–7.302.III.B of the Attorney General Memorandum dated 30 May 2002, cannot be reached, authorization may be given by the Commander, CID or designee.

*(b)* The Commander, CID must notify the OEO as soon as practicable after the emergency interception is authorized, but not later than 3 working days after the authorization. The notification explains the emergency and contains the information required in paragraph 2–1 of this regulation.

(2) The Commander, CID, or designee, may orally grant an emergency request in which written DOJ approval is not required for a consensual intercept, for a period not to exceed 10 days. The criminal investigator prepares and submits the written request required in paragraph 2–1 of this regulation to the Commander, CID, within 48 hours of receiving oral authorization for an emergency consensual interception. The Commander, CID, or designee, may approve the emergency request under the following conditions:

*(a)* A person's life or physical safety is reasonably believed to be in immediate danger, and the information captured by the interception is likely to alleviate the danger.

*(b)* The physical security of a DOD installation or other significant U.S. Government property is reasonably believed to be in immediate danger, and the information captured by the interception is likely to alleviate the danger.

*(c)* Evidence of significant criminal conduct is likely to be lost before a written request for consensual interception can be processed.

*(d)* The security or execution of a U.S. military operation is believed to be threatened or U.S. security interests will be jeopardized and the information captured by the interception is likely to alleviate the threat.

## Chapter 4
## Procedures Governing the Use of Pen Registers and Similar Devices or Techniques

### 4–1. General
The procedures of this chapter apply to the use of pen registers and similar devices.

### 4–2. Approval
Pen register operations are approved by the same authorities and in the same manner, subject to the same restrictions, as consensual interceptions under the provisions of paragraph 2–1 of this regulation. A pen register operation will not be authorized if it would violate the relevant SOFA or the applicable domestic law of the host nation. The request for approval to conduct a pen register operation will include the following information:

*a.* The identity of the CID special agent making the application.

*b.* A complete statement of the facts and circumstances that support the applicant's assertion that there is probable cause to believe that the operation will produce evidence of a crime. The statement should include a description of the offense involved, a description of the nature and location of the facilities from which the intercepted information originates, and the identity of the person, if known, who has committed, is about to commit, or is committing the offense and who is the target of the operation.

*c.* A statement of the period of time for which the operation is required to be maintained.

*d.* The statement that, in judgment of the person making the request, the operation is warranted in the interest of effective law enforcement.

### 4–3. Pen registers and trap and trace devices in the United States and its territories
*a.* Except when the consent of the user is 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 is obtained, in accordance with 18 USC Chapter 206.

*b.* A notice to all users (for example, through banners or computer user agreements) that a device is to be installed on electronic communication lines located on DOD installations or under DOD jurisdiction is construed as user consent.

*c.* If notice to all users is not given because it would result in an undesired effect on the investigation (for example, it would alert a target of the fact of an investigation), a court order must be obtained.

*d.* Where the consent of the user has not been obtained, the following procedures are 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 DOJ makes an application in writing and under oath or equivalent affirmation to a court of competent jurisdiction for an order authorizing or approving the installation and use of a pen register or trap and trace device.

(2) The application includes 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 is requested in accordance with 18 USC 3125 through coordination with the local U.S. Attorney or the OEO, DOJ.

*e.* All requests for pen registers and trap and trace devices will be approved in accordance with paragraph 2–1 of this regulation prior to seeking a court order.

### 4–4. Pen registers and trap and trace devices outside the United States and its territories
*a.* If the target of the law enforcement investigation is subject to the UCMJ and trial by court-martial may result, before an order may be issued, a military judge assigned to receive such application by TJAG, pursuant to this instruction, must find that the contemplated use and installation of a pen register or trap and trace device does not violate host country laws, any applicable SOFA, or any other agreement with the host country.

*b.* In those cases where the target of the law enforcement investigation is subject to federal prosecution under the MEJA or other possible prosecution in federal district courts, the criminal investigator consults with the servicing JA (or other appropriate legal counsel) and the DOJ to ensure that the installation of such devices is permitted in accordance with U.S. laws and does not violate host country laws, any applicable SOFA, or other agreement with host country authorities.

*c.* If the target of the law enforcement investigation is not subject to the UCMJ or federal prosecution under the MEJA or other possible prosecution in the federal district court, the investigative component consults with the servicing SJA (or other appropriate legal counsel) and the DOJ to ensure that the installation of such devices is in accordance with host country laws, any applicable SOFA, and any other agreement with the host country.

*d.* Approval for emergency authorizations of operations will be telephonically requested through the Commander, CID or designee.

*e.* All requests for pen registers and trap and trace devices will be approved in accordance with paragraph 3–2 of this regulation prior to seeking a court order.

### 4–5. Pen register operations which include nonconsensual interceptions of wire communications

When an operation using the procedures outlined in paragraphs 4–1 through 4–4 will be conducted in conjunction with a nonconsensual interception of a wire communication as described in paragraph 3–1 of this regulation, the procedures listed in paragraph 3–1 will apply to the entire operation.

### 4–6. Global Positioning Systems and tracking devices

The use of GPS or cellular devices with tracking capability may be used as an investigative tool only after consulting with the servicing trial counsel or the DOJ trial attorney or AUSA, depending upon whether the case is prosecuted in the military justice system or civilian court system, to identify the legal implications and requirements for this technology.

## Chapter 5
## Procedures Governing Telephone Tracing

### 5–1. General

When prior consent of one or more parties to a telephone tracing operation, including cellular phones, has been obtained, the use of tracing equipment and techniques will be authorized only after coordination with appropriate JA personnel or other appropriate legal counsel.

### 5–2. Tracing approval

*a.* To conduct consensual trap and trace operations on a military installation of a U.S. Government owned or leased line, the requesting CID field element will submit a request to the installation commander, who will decide whether or not to approve the operation after coordinating with the servicing SJA.

*b.* To conduct consensual trap and trace operations of a residential line on a military installation, the requesting CID field element will obtain written consent of the user. Upon receipt of the written consent, coordination will be made with the servicing JA to determine if further approval is necessary. In the continental United States, written consent from the user to the servicing telephone company is normally all that is required. Outside the continental United States (OCONUS), the written consent may require concurrence of the installation commander.

*c.* For consensual trap and trace operations on military installations abroad, the operation must respect applicable SOFA and foreign law.

*d.* For consensual trap and trace operations outside military jurisdiction, the CID field element will coordinate with the local civilian or host country authorities when appropriate for approvals.

## Chapter 6
## Interception Equipment

### 6–1. Control of interception equipment

*a.* In accordance with DODI O–5505.09, the only DA law enforcement activity authorized to procure or maintain equipment primarily used for the interception of wire and oral communications described in this regulation is the CID. The U.S. Army Military Police School may acquire, possess, or use such equipment for training purposes only. Such equipment, considered technical listening equipment (TLE), consists of devices and items of equipment designed

primarily or used for wiretap, investigative monitoring, or eavesdrop activities. This equipment does not include items such as common audio or video recorders, cellular phones, equipment normally available to telephone/signal facilities or activities, or other equipment not primarily designed or used for the interception of wire or oral communications. Items of equipment with an interception capability permanently installed as part of an Army leased, owned, or operated telephone/signal facility are exempted from the controls of this chapter; however, their use to intercept wire or oral communications for law enforcement purposes will be as prescribed by this regulation.

*b.* TLE will be safeguarded to prevent unauthorized access or use, with appropriate inventory records to account for all equipment at all times. Equipment will be returned to storage when not in actual use, except to the extent that returning the equipment would interfere with its proper utilization.

*c.* Copies of the completed inventories of equipment will be retained in accordance with AR 735–5.

### 6–2. Disposal of interception equipment

*a.* Federal law prohibits the sale or possession 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 or oral communications..." Accordingly, disposal outside the Government of such interception equipment is prohibited.

*b.* TLE must be transferred to an agency authorized to use it or destroyed.

*c.* If there is any question as to what purpose an item of equipment is primarily useful for, then the officials involved should, in the exercise of due caution, prohibit its sale pending referral to the DOD General Counsel for a determination as to the proper classification of such devices under the law.

## Chapter 7
## Access to Electronic Communications in Electronic Storage or in a Remote Computing Service; Records Concerning Electronic Communication Service or Remote Computing Service

### 7–1. General

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 components for law enforcement in the United States and its territories is obtained in accordance with 18 USC 2703. This does not apply to government owned and operated computer networks not providing services to the public.

### 7–2. 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 (available at http://www.uscourts.gov/rules-policies) or equivalent state warrant.

*b.* Access to the contents of an electronic communication held in electronic storage for more than 180 days will be obtained by:

(1) Warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant without prior to notice being given to the subscriber or customer.

(2) Court order or administrative subpoena with prior notice given to the subscriber or customer.

### 7–3. Electronic communications held in a remote computing service

*a.* Access to the contents of an electronic communication held in or maintained by a remote computing service will be obtained in accordance with 18 USC 2703.

*b.* If notice is not given to the subscriber or customer of the remote computing service, a warrant is obtained.

*c.* If notice is provided to the subscriber or customer of the remote computing service, access may be obtained by administrative subpoena authorized by a federal or state statute, federal or state grand jury or trial subpoena, or by court order.

*d.* Access to basic subscriber information may be obtained by administrative subpoena authorized by a federal or state statute, federal or state grand jury or trial subpoena, or by court order.

### 7–4. 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 may be obtained—

*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 7–2*b*(1) of this regulation.

*c.* By court order consistent with 18 USC 2703(b).

*d.* With the consent of the subscriber or customer.

## Chapter 8
## Records Administration

### 8–1. General

All recordings and records of information obtained through interception activities conducted under the provisions of this regulation will be safeguarded in the investigative file to preclude unauthorized access, theft, or use. Both the interest of the government and the rights of private individuals involved will be considered in the development of safeguarding procedures. Storage and access requirements for applications, orders, recordings, and other records of information obtained through interception activities will be as prescribed in AR 190–45, AR 195–2, AR 25–55, and AR 25–400–2.

### 8–2. Records requirements

*a.* All records pertaining to consensual and nonconsensual interceptions, to include denied and unexecuted applications, are to be maintained in the permanent investigative case files and are not destroyed earlier than required by this regulation, even if the investigative file may otherwise be destroyed in accordance with normal destruction procedures. Recordings of the interceptions made in the United States and its territories pursuant to 18 USC 2518 may be destroyed only upon an order of the court involved, and must be maintained for at least 10 years.

*b.* Records of all interception applications submitted to and disapproved by a United States District Court or military judge for authorization for a nonconsensual interception of a wire, electronic, or oral communication are preserved and maintained in the investigative file and include—

(1) Available identifying data for each reasonably identifiable target of the applied-for interception.

(2) Telephone numbers or radio telephone call signs involved in the application.

(3) City, state, and judicial district of the interception, and, if known, address(es) of the location or the applied-for interception.

(4) Case number or other identifier for the application.

(5) Statement of the other facts about the application, the reason the application was refused, and a brief explanation of why the interception was not done.

*c.* The approving authority for one party consensual interception requests will maintain records of all approved and denied authorizations to conduct consensual interceptions and include the purpose for the denial.

### 8–3. Dissemination controls

*a.* All recordings and records of information obtained though interception activities pursuant to this regulation will be used only as required to satisfy the requirements of 18 USC 2518 (statement of prior applications).

*b.* In all cases access to information obtained by interception activities conducted under the provisions of this regulation will be restricted to those individuals having a defined need-to-know clearly related to the performance of their duties.

*c.* The information may be disseminated outside the DOD only when—

(1) Required for the purposes described in 18 USC 2517.

(2) Required by law (including the Privacy Act of 1974, as amended, and the Freedom of Information Act of 1967, as amended), or order of a Federal court.

(3) Requested by a committee of the Congress and approved for release by the DOD General Counsel.

(4) Required by the provisions of SOFA or other international agreements.

*d.* Dissemination of the information described above will be controlled in accordance with AR 190–45; AR 195–2; AR 25–55; and AR 25–22 as appropriate. Procedures will, in all circumstances, include sufficient records to provide an accurate audit trail reflecting dissemination of this information.

### 8–4. Retention and disposition of records

Notwithstanding the provisions of paragraph 8–1, records and recordings of interceptions will be retained for at least 10 years after termination of the interception prior to disposal in accordance with appropriate records retirement

procedures. Additionally, if the interception was conducted in the United States under the provisions of 18 USC 2516, the records may be destroyed only pursuant to an order of the court involved.

# Appendix A

# References

## Section I

### Required Publications

Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (https://armypubs.army.mil). USC publications are available at https://www.gpo.gov/fdsys/.

**AR 190–45**
Law Enforcement Reporting (Cited in para 8–1.)

**AR 195–2**
Criminal Investigation Activities (Cited on title page.)

**AR 735–5**
Property Accountability Policies (Cited in para 6–1*c*.)

**Attorney General Memorandum dated 30 May 2002**
Procedures for Lawful, Warrantless Monitoring of Verbal Communications (Cited in para 3–5*b*(1).) (Available at http://www.justice.gov/sites/default/files/ag/legacy/2009/02/10/ag-053002.pdf.)

**18 USC Chapter 119**
Wire and Electronic Communications Interception and Interception of Oral Communications (Cited in para 1–4*c*.)

**18 USC Chapter 206**
Pen Registers and Trap and Trace Devices (Cited in para 4–3*a*.)

## Section II

### Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website (https://armypubs.army.mil). USC material is available at https://www.gpo.gov/fdsys/. The UCMJ is available at http://www.ucmj.us/.

**AR 11–2**
Managers' Internal Control Program

**AR 25–1**
Army Information Technology

**AR 25–22**
Army Privacy Program

**AR 25–30**
Army Publishing Program

**AR 25–55**
The Department of the Army Freedom of Information Act Program

**AR 25–400–2**
The Army Records Information Management System (ARIMS)

**AR 190–30**
Military Police Investigations

**AR 195–5**
Evidence Procedures

**AR 380–53**
Communications Security Monitoring

**AR 381–10**
U.S. Army Intelligence Activities

**AR 381–14**
Technical Surveillance Countermeasures

**AR 381–20**
Army Counterintelligence Program

**DODI O–5505.09**
Interception of Wire, Electronic, and Oral Communications for Law Enforcement (Available at http://www.dtic.mil/whs/directives/.)

**Manual for Courts–Martial**
Manual for Courts-Martial, United States (2012 Edition) (Available at http://jsc.defense.gov/military-law/current-publications-and-updates/.)

**UCMJ Art. 15**
Commanding Officer's Non-Judicial Punishment

**UCMJ Art. 26**
Military Judge of a General or Special Court-Martial

**UCMJ Art. 32**
Investigation

**USAM, Title 9, Criminal Resource Manual 625**
Federal Rule of Criminal Procedure 11(e) (Available at https://www.justice.gov/usam/criminal-resource-manual-625-federal-rule-criminal-procedure-11e.)

**18 USC 2510**
Definitions

**18 USC 2516**
Authorization for interception of wire, oral, or electronic communications

**18 USC 2517**
Authorization for disclosure and use of intercepted wire, oral, or electronic communications

**18 USC 2518**
Procedure for interception of wire, oral, or electronic communications

**18 USC 2703**
Required disclosure of customer communications or records

**18 USC 3125**
Emergency pen register and trap and trace device installation

## Section III

## Prescribed Forms

This section contains no entries.

## Section IV

## Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

**DA Form 11–2**
Internal Control Evaluation Certification

**DA Form 2028**
Recommended Changes to Publications and Blank Forms

## Appendix B

## Internal Control Evaluation

### B–1. Function
The function covered by this evaluation is evidence procedures.

### B–2. Purpose
The purpose of this evaluation is to assist CID supervisors, commanders, and inspectors in evaluating the key internal controls listed and determining if proper TLE procedures are being employed.

### B–3. Instructions
Answers must be based on the actual testing of key internal controls (for example, document analysis or direct observation). Answers that indicate deficiencies must be explained and the corrective action identified in supporting documentation. These internal controls must be evaluated at least once every 5 years. Certification that the evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

### B–4. Test questions
*a.* Are special agents aware of the process to request authorization to employ TLE without the consent of any party to the communication?

*b.* Were consensual interception requests submitted to the appropriate approval authority?

*c.* Was local legal coordination made before consensual interception requests were submitted to the approval authority?

*d.* Are records pertaining to all interceptions maintained in the investigative file?

*e.* Are records maintained for the time period specified in this regulation and DODI O–5505.09?

*f.* Is TLE being stored in a secured location?

*g.* Are records being maintained for the use of TLE?

*h.* Are special agents trained on the use of TLE to include all applicable laws governing the use?

### B–5. Suppression
Not applicable.

### B–6. Comments
Help make this a better tool for evaluating internal controls. Submit comments to the Director, U.S. Army Criminal Investigation Division, via email to usarmy.belvoir.hqda-usacid.mbx.cidpolicy@army.mil.

## Glossary

### Section I

### Abbreviations

**AR**
Army regulation

**AUSA**
Assistant U.S. Attorney

**CID**
Criminal Investigation Division

**DA**
Department of the Army

**DOD**
Department of Defense

**DODI**
Department of Defense instruction

**DOJ**
Department of Justice

**GPS**
Global Positioning Systems

**HQ**
Headquarters

**ID**
identification

**JA**
judge advocate

**MEJA**
Military Extraterritorial Jurisdiction Act

**OCONUS**
outside the continental United States

**OEO**
Office of Enforcement Operations

**SAUSA**
Special Assistant U.S. Attorney

**SJA**
Staff Judge Advocate

**SOFA**
Status of Forces Agreement

**TJAG**
The Judge Advocate General

**TLE**
technical listening equipment

**UCMJ**
Uniformed Code of Military Justice

**USAM**
U.S. Attorney's Manual

**USC**
United States Code

## Section II

## Terms

The definitions of terms applicable to this regulation are as follows. See AR 190–45, AR 195–2, and DODI O–5505.09 for other applicable terms.

**Abroad**
OCONUS. An interception takes place abroad when the interceptive device is located and operated outside the United States and the target of the interception is located OCONUS.

**Application for court order**
A document containing specified information prepared for and forwarded to a judge of the U.S. District Court or the U.S. Court of Appeals, or a military judge.

**Army law enforcement**
Military Police, DA Police and CID Special Agents, and investigative personnel.

**Consensual interception**
An interception of a wire or oral communication after verbal or written consent for the interception is given by one or more of the parties to the communication.

**Consensual monitoring**
Listening to a telephone conversation, with or without a telephone extension instrument, where one party of the conversation consents to the monitoring for a valid law enforcement purpose. Such monitoring is not considered an interception of wire or oral communication; however, any recordings of conversations under these circumstances must comply with paragraph 2–1 of this regulation.

**Court order**
An order issued by a judge of a U.S. District Court or a U.S. Court of Appeals or by a military judge authorizing a wire or oral interception or a pen register operation.

**Interception**
The aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device. The term "contents" includes any information concerning the identity of the parties of such communication or the existence, substance, purpose, or meaning of that communication. See 18 USC 2510.

**Oral communication**
Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception, under circumstances justifying such expectations. See 18 USC 2510.

**Pen register**
A device connected to a telephone instrument or line that permits the recording of telephone numbers dialed from a particular telephone instrument. "Pen register" also includes decoder devices used to record the numbers dialed from a touchtone telephone. "Pen register" does not include equipment used to record the numbers dialed for and duration of long-distance telephone calls when the equipment is used to make such records for an entire telephone system and for billing or communications management purposes.

**Technical listening equipment (electronic, mechanical, or other device)**
Any device or apparatus that can be used to intercept a wire or oral communication, other than any telephone equipment (including extensions) furnished to the subscriber or user by a communications common carrier or an Army leased, owned, or operated facility in the ordinary course of its business, and used by the subscriber or user in the ordinary course of its business or used by an investigative or law enforcement officer in the ordinary course of duty. See 18 USC 2510.

**Telephone tracing**
A technique or procedure to determine the origin, by telephone number and location, of a telephone call made to a known telephone instrument. The terms "lock-out" and "trapping" may also be used to describe this technique.

**United States**
For the purpose of this regulation the term United States includes the 50 States of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States.

**United States person**
For purposes of this regulation, a United States citizen, an alien admitted to the United States for permanent residence, a corporation incorporated in the United States, or an unincorporated association organized in the United States and substantially composed of United States citizens or aliens admitted to the United States for permanent residence.

**Wire communication**
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 or by an Army leased, owned, or operated facility in providing or operating such facilities for the transmission of interstate or foreign communications. See 18 USC 2510.

## Section III

## Special Abbreviations and Terms
This section contains no entries.