DoD INSTRUCTION 5505.09

COMMUNICATION INTERCEPTION FOR LAW ENFORCEMENT

Originating Component:	Office of Inspector General of the Department of Defense
Effective:	August 22, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction O-5505.09, "Interception of Wire, Electronic, and Oral Communications for Law Enforcement," November 27, 2013, as amended
Approved by:	Robert P. Storch, Inspector General of the Department of Defense

Purpose: In accordance with the authority in DoD Directive 5106.01, this issuance establishes policy, assigns responsibilities, and prescribes procedures for intercepting wire, electronic, and oral communications for law enforcement in accordance with Sections 2510-2523 and 3121-3127 of Title 18, United States Code (U.S.C.).

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 4
1.1. Applicability. 4
1.2. Policy. 5
SECTION 2: RESPONSIBILITIES 7
2.1. IG DoD. 7
2.2. Secretaries of the Military Departments. 7
2.3. The IG DoD and the Secretaries of the Military Departments. 7
SECTION 3: PROCEDURES 8
3.1. Request for Consensual Intercepts. 8
a. The IG DoD and Secretaries of the Military Departments: 8
b. The Directors and Commanders of the DCIOs: 8
3.2. Consensual Intercepts of Communications. 9
a. Consensual Interception of Oral Communication. 9
b. Oral Communication Interception Requiring Prior Written U.S. Department of Justice (DOJ) Approval. 11
c. Emergency Authorization. 12
d. Consensual Interception of Wire Communication. 13
e. Consensual Interception of Electronic Communication. 13
3.3. Nonconsensual Intercepts. 13
a. In the United States and Its Territories. 13
b. Outside the United States and Its Territories. 13
3.4. Pen Registers and Trap and Trace Devices in the United States and Its Territories. 15
3.5. Pen Registers and Trap and Trace Devices Outside the United States and Its Territories. 16
3.6. Mobile Tracking Devices. 16
3.7. Access to, or Records Concerning, Electronic Communications in Electronic Storage or in a Remote Computing Service. 17
a. Electronic Communications Held in Electronic Storage 17
b. Records Concerning Electronic Communication Service or Remote Computing Service. 17
c. Prospective Location Records Concerning Electronic Communication Service. 17
SECTION 4: RECORDS 19
4.1. General. 19
4.2. Requirements. 19
4.3. Denied Interception Applications. 19
4.4. Interception Application Approved But Not Executed. 19
4.5. Retention. 20
4.6. Dissemination Controls. 20
4.7. Retention and Disposition. 20
SECTION 5: INTERCEPTION EQUIPMENT 21
5.1. Control. 21
5.2. Disposal. 21
GLOSSARY 22

G.1. Acronyms. 22
G.2. Definitions. 22
REFERENCES 24

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

b. To support law enforcement actions, applies to:

(1) Intercepting wire, electronic, and oral communications.

(2) Using individual global positioning system tracking devices.

c. Does not apply to:

(1) Intercepting wire, electronic, and oral communications for counterintelligence or foreign intelligence, including information on the foreign aspects of narcotics production and trafficking, in accordance with Executive Order 12333 and DoD Manual 5240.01.

(2) National Security Agency activities and the cryptologic elements of the Military Departments.

(3) Communications security activities authorized pursuant to DoD Instructions (DoDIs) 5240.05, 8523.01, and 8560.01.

(4) Installation of a pen register or trap and trace device on electronic communications lines on DoD property or under DoD jurisdiction for non-law enforcement activities.

(5) Interceptions arising from:

(a) Technical surveillance countermeasures activities authorized pursuant to Executive Order 12333.

(b) Readily apparent video or audio equipment installed in DoD traffic or law enforcement patrol vehicles operating on DoD property or within DoD jurisdiction.

(c) Readily apparent video or audio equipment worn on the body of DoD law enforcement or security personnel operating on DoD property or within DoD jurisdiction.

(d) Readily apparent video or audio equipment to record law enforcement interrogations and interviews.

(6) Intercepting wire, oral, or electronic communications in accordance with Section 2511(2)(a)(i) of Title 18, U.S.C.

d. Does not modify or supersede status-of-forces or other specific agreements that may otherwise limit implementation in any particular geographical area abroad.

e. Does not create any right or benefit, substantive or procedural, enforceable by law against the United States or the DoD or its officers, employees, or agents.

f. Nothing in this instruction will infringe on the IG DoD's statutory independence and authority in accordance with Chapter 4 of Title 5, U.S.C., also known and referred to in this issuance as the "Inspector General Act of 1978," as amended. In the event of any conflict between this instruction and the IG DoD's statutory independence and authority, the Inspector General Act of 1978 will take precedence.

1.2. POLICY.

a. The Defense Criminal Investigative Organizations (DCIOs) use approved interception techniques when prudent and necessary to develop evidence relevant to their investigations.

b. The DCIOs may procure and maintain equipment primarily designed for intercepting wire, electronic, and oral communications; pen registers; and trap and trace devices for law enforcement purposes. Use of such equipment for law enforcement is prohibited unless done in accordance with this instruction and Sections 2510-2523 and 3121-3127 of Title 18, U.S.C.

c. Nonconsensual interception of wire, electronic, and oral communications for law enforcement purposes will not be treated as normal or routine investigative procedures. Nonconsensual intercepts may be requested only when investigators can demonstrate that the information is necessary and cannot otherwise be reasonably obtained.

d. Only the DCIO's criminal investigators may engage in the nonconsensual interception of wire, electronic, and oral communications and the use of pen register and trap and trace devices for law enforcement purposes. Confidential human sources or cooperating witnesses under the control and supervision of a criminal investigator are an extension of criminal investigators' nonconsensual interception activity; therefore, such action is authorized.

(1) Intercepting and using pen register and trap and trace devices will be in accordance with this instruction and the statutory provisions of Sections 2510-2523 and 3121-3127 of Title 18, U.S.C.

(2) Intercepting and using pen register and trap and trace devices by other DoD personnel, employees, or contractors who are not under the control and supervision of a criminal investigator is prohibited, except activities authorized by Sections 2510-2523 and 3121-3127 of Title 18, U.S.C., for service providers.

e. Delegating approval authority for interceptions is not mandatory, but, if delegated, must be in accordance with this instruction.

f. When conducting interception activities pursuant to this instruction, the privacy of the individual must be respected to the maximum extent consistent with the interception activities. When applicable, any information collected will be protected by, and maintained in accordance with, DoDI 5400.11.

g. Personally identifiable information collected and used in executing this instruction must be safeguarded to prevent any unauthorized use. Collection, disclosure, and release of personally identifiable information must comply with the requirements of DoD 5400.11-R and DoDI 5505.17.

SECTION 2: RESPONSIBILITIES

2.1. IG DOD.

In addition to the responsibilities in Paragraph 2.3., the IG DoD monitors and evaluates compliance with this instruction.

2.2. SECRETARIES OF THE MILITARY DEPARTMENTS.

In addition to the responsibilities in Paragraph 2.3., the Secretaries of the Military Departments:

a. Ensure military judges are designated by the Judge Advocate General in the respective Military Department to administer the appropriate functions assigned in Section 3.

b. Provide a copy of each policy implemented pursuant to this instruction to the IG DoD.

2.3. THE IG DOD AND THE SECRETARIES OF THE MILITARY DEPARTMENTS.

The IG DoD and the Secretaries of the Military Departments, in their respective areas of responsibility, prescribe and monitor procedures for DCIO heads to implement this instruction and comply with Section 3.

SECTION 3: PROCEDURES

3.1. REQUEST FOR CONSENSUAL INTERCEPTS.

a. The IG DoD and Secretaries of the Military Departments:

(1) Authorize the consensual interception or seeking of judicial authorization for nonconsensual interception of wire, electronic, and oral communications for law enforcement following legal review and concurrence in accordance with this instruction and Sections 2510-2523 and 3121-3127 of Title 18, U.S.C.

(2) May delegate this authority in writing and ensure the designee is a DCIO director, commander, or headquarters-level deputy director, vice commander, or deputy commander who directly oversees criminal investigative operations.

(a) Such authority may also be delegated to a person serving in a Senior Executive Service, general officer/flag officer, or regional commander or director position that directly oversees criminal investigations, provided the designee seeks staff judge advocate (SJA) or legal counsel review of the intercept request before approving.

(b) Authority to approve only telephonic consensual intercepts can also be delegated to special agents in charge, provided the designee seeks SJA or legal counsel review of the intercept request before approving.

(3) Furnish the list of designations made in Paragraphs 3.1.a.(1) and 3.1.a.(2) to the IG DoD for Investigative Oversight and Special Investigations and Reviews.

b. The Directors and Commanders of the DCIOs:

(1) Issue regulations specifying special storage and access requirements for applications, orders, recordings, and other records 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.

(2) Develop regulations, policies, and procedural controls and designate responsible officials for internally and externally disseminating the information. Procedures require creating and maintaining records reflecting dissemination of that information.

(3) Establish and maintain the records and other information required in Section 4.

(4) Establish procurement controls and maintain interception equipment, as required by Section 5.

(5) Train personnel involved in the activities and techniques discussed in Section 3 in applicable requirements and controls, including awareness of the criminal and civil sanctions for illegally intercepting wire, electronic, and oral communications.

3.2. CONSENSUAL INTERCEPTS OF COMMUNICATIONS.

a. Consensual Interception of Oral Communication.

The May 30, 2002 Attorney General Memorandum established requirements for the consensual interception of oral communications.

(1) A DCIO criminal investigator must request written approval from the delegated DoD Component approval authority, as specified in Paragraph 3.1.a., before engaging in a consensual interception of oral communication.

(2) The criminal investigator must prepare a written request that includes at least:

(a) Background of the Investigation.

Provide a detailed background of the investigation and the need for the interception.

(b) Reason for the Interception.

1. If the interception is for investigative purposes, cite the criminal statute involved.

2. If the interception is intended to provide protection to the consenting party, explain the nature of the danger to the consenting party.

(c) Location and Type of Device.

Describe the type of device to be used, along with a description of where the device will be hidden (e.g., on the person, in personal effects, or in a fixed location).

(d) Location of Interception.

Provide the physical location and primary Federal jurisdiction where the interception will take place. If the location changes, the criminal investigator must promptly provide written notice to the approving official.

(e) Time.

1. Provide the length of time needed to intercept and get the necessary information.

2. An authorization may be granted for up to 90 days from the date the interception is scheduled to begin. An authorization to intercept may be renewed for 90 day periods upon reapplication.

3. In special cases, such as in a DCIO run or supervised undercover operation that is expected to last at least 180 days or when an undercover agent portrays an identity other than their own or uses alias personas to assume a role in criminal activity, an authorization for up

to 180 days may be granted. A special case authorization may be renewed for 180 day periods upon reapplication

(f) Names.

1. Provide the names of persons, if known, whose communications are expected to be intercepted and their relation to the investigation or the need for the interception.

2. Identify whether the persons are consenting or non-consenting parties to the intercept. If the consent is not obtained in writing, submit a statement on how consent was obtained.

3. Names of undercover operatives, cooperating citizens, or informants may be identified by an individualized informant or source number.

(g) Attorney Advice.

Provide a statement that the facts of the interception have been discussed with the Assistant U.S. Attorney, supporting SJA, or legal counsel associated with the particular investigation, the date of that discussion, and whether:

1. That Assistant U.S. Attorney, supporting SJA, or legal counsel believes that the use of consensual interception is appropriate.

2. The use amounts to entrapment as decided in governing case law.

(3) A request to renew authority to intercept must contain all the information required for the initial request. The DCIO criminal investigator must submit the request to the delegated DoD Component approval authority for approval. The renewal request must also:

(a) Refer to all previous authorizations.

(b) Explain why additional authorization is needed.

(c) Provide updated attorney advice on the renewal request as required by Paragraph 3.2.a.(2)(g).

(4) Excluding any exceptions noted elsewhere in this instruction (e.g., emergency situations, joint investigations), consensual interceptions of wire, electronic, and oral communications will be authorized in writing by the DCIO approval authority or their designee, after a legal sufficiency review. The DCIO approval authority will maintain the determination in the DCIO's filing system.

(5) A DCIO 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:

(a) DoD personnel participate in the monitoring,

(b) DCIO equipment is used in the monitoring; or

(c) The monitoring takes place on a DoD installation.

(6) With the consent of one of the parties to a telephone conversation, DCIO criminal investigators may use a telephone extension to listen to a conversation, without recording it with interception equipment, for law enforcement purposes without the need for approval.

(7) With the consent of one of the parties to a text messaging exchange or social media interaction, DCIO criminal investigators may monitor the communication activity, without recording it with interception equipment, in real time for law enforcement purposes without the need for approval.

b. Oral Communication Interception Requiring Prior Written U.S. Department of Justice (DOJ) Approval.

(1) Requests for written authorization from the DOJ, Office of Enforcement Operations, to monitor an oral communication with the consent by at least one party but not all parties, using interception recording equipment, must contain the information described in Paragraph 3.2.a.(2). Requests will be sent to:

U.S. Department of Justice
Attn: Director, Office of Enforcement Operations
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
Fax# (202) 514-6809

(2) The Director or Associate Director, Office of Enforcement Operations, DOJ, must approve the request and must be notified when:

(a) The monitoring relates to an investigation of:

1. A member of Congress.

2. A Federal judge.

3. A member of the Executive Branch at Executive Level IV or above.

4. A person who has served in such capacity within the previous 2 years.

(b) The monitoring relates to an investigation involving bribery, conflict of interest, or extortion relating to performing the official duties of a:

1. Governor, lieutenant governor, or attorney general of any State or territory; or

2. Judge or justice of the highest court of any State or territory.

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

(d) Any party to the communication is, or has been, a member of the U.S. Marshals Service Witness Security Program and that fact is known to the agency involved or its officers.

(e) The consenting or non-consenting person is in the custody of the Federal Bureau of Prisons or the U.S. Marshals Service.

(f) 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.

(3) Written requests for authorization to intercept under any of these sensitive circumstances will be approved by the DoD Component approval authority then submitted by the Component general counsel, or designee, to the Director or Associate Director, Office of Enforcement Operations, DOJ for review and processing.

c. Emergency Authorization.

(1) An emergency request for a consensual intercept, in which written DOJ approval is required, may be made by telephone to the DOJ approval officials listed in Part III.B of the May 30, 2002 Attorney General Memorandum by a criminal investigator after review by the Component general counsel and approval by the DoD Component approval authority or their designee.

(a) The criminal investigator must put the request in writing and submit it to the DoD Component approval authority as soon as practicable, after authorization has been obtained. If the officials listed in Part III.B of the May 30, 2002 Attorney General Memorandum cannot be reached, the DoD Component head or their designee may authorize the request.

(b) The Component must notify the Director or Associate Director, Office of Enforcement Operations, DOJ, within 3 working days after the authorization. The notification must explain the emergency and include the information required by Paragraph 3.2.a.(2).

(2) The DoD Component approval authority may orally grant an emergency request in which written DOJ approval is not required for a consensual intercept, for a period no longer than 10 calendar days. The criminal investigator must prepare and submit the written request required in Paragraph 3.2.a.(2) to the DoD Component approval authority within 48 hours after receiving oral authorization for an emergency consensual interception. The Component approval authority may approve the emergency request when:

(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) Critical evidence of criminal conduct is likely to be lost before a written request for consensual interception can be processed; or

(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.

d. Consensual Interception of Wire Communication.

Procedures for requesting and approving consensual interception of wire communications are the same as those for consensual interception of oral communication as described in Paragraph 3.2.a.(2), with the exception that, in addition to describing the device to be used in accordance with Paragraph 3.2.a.(2)(d), a description of the type and location of the communication sought to be intercepted must also be included.

e. Consensual Interception of Electronic Communication.

(1) DCIO heads or their designees may authorize intercepting electronic communications when one of the parties to the communication gives consent.

(2) For all other requests to intercept electronic communications, criminal investigators must consult with the local U.S. attorney's office or the DOJ. If the targeted individual is subject to Chapter 47 of Title 10, U.S.C., also known and referred to in this instruction as the "Uniform Code of Military Justice (UCMJ)," criminal investigators must consult with the supporting SJA.

3.3. NONCONSENSUAL INTERCEPTS.

a. In the United States and Its Territories.

(1) Nonconsensual interception of wire, electronic, and oral communications, and the audio portion of video monitoring, for law enforcement is permitted in the United States and its territories only after a court order has been obtained, in accordance with Section 2518 of Title 18, U.S.C., and only for the offenses enumerated in Section 2516 of Title 18, U.S.C.

(2) In accordance with procedures adopted by each organization, the DCIO heads or their designees may directly request of the appropriate authority (e.g., local U.S. attorney's office) the preparation and presentation of an application for a court order to proper judicial authority. The DCIO criminal investigators will provide such assistance to the requesting authority (e.g., local U.S. attorney's office), as required.

b. Outside the United States and Its Territories.

(1) When the target of the law enforcement investigation is subject to the UCMJ:

(a) An authorization application will 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.

(b) Authorization applications issued by military judges must contain the information required by Section 2518(1) of Title 18, U.S.C. and may contain the information required by Section 2518(2) of Title 18, U.S.C.

(c) The military judge may enter an *ex parte* authorization, as requested or modified, authorizing or approving intercepting wire, electronic, or oral communications by the DCIO concerned if, on the basis of the application and other information provided by the requesting agency, the military judge determines that:

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

2. There is probable cause to believe that particular communications about that offense will be obtained through such interception.

3. Normal investigative procedures have been tried and have failed, or reasonably appear to be either unlikely to succeed or too dangerous if tried.

4. Except as provided in Section 2518(11) of Title 18, U.S.C., 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 to commit the offense under investigation, are owned by, leased to, listed in the name of, or commonly used by, a person subject to the UCMJ.

5. The interception is consistent with U.S. laws, and the interception does not violate host country laws, any applicable status-of-forces agreement, or other agreement with the host country.

6. Each authorization of the interception complies with the requirements of Sections 2518(4) and 2518(5) of Title 18, U.S.C., 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 Section 2518(5) of Title 18, U.S.C.

(2) When the target of the law enforcement investigation is subject to Federal prosecution pursuant to Chapter 212 of Title 18, U.S.C., also known and referred to in this instruction as the "Military Extraterritorial Jurisdiction Act," or other possible prosecution in Federal district courts, the investigative component will ensure that:

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

(b) The interception does not violate host country laws, any applicable status-of-forces agreement, or other agreement with host country authorities.

(c) The target's rights, as applicable, under the Fourth Amendment to the United States Constitution are not infringed. The supporting SJA (or other appropriate legal counsel) and the DOJ Office of International Affairs will be consulted.

(3) When the target of the law enforcement investigation is not subject to the UCMJ or Federal prosecution pursuant to the Military Extraterritorial Jurisdiction Act or other possible prosecution in Federal district courts, nonconsensual interceptions of wire, electronic, and oral communications will be permitted only in accordance with host country laws, any applicable status-of-forces agreement, and any other agreement with the host country.

(4) When an emergency situation exists as described in Section 2518(7)(a) of Title 18, U.S.C., and there is not sufficient time to obtain an authorization, the DoD Component head concerned may authorize emergency interception of a wire, electronic, or oral communication, but must then notify the Director or Assistant Director, Office of Enforcement Operations, DOJ, within 48 hours.

3.4. PEN REGISTERS AND TRAP AND TRACE DEVICES IN THE UNITED STATES AND ITS TERRITORIES.

a. Except when the consent of the user is obtained, installing and using a pen register or trap and trace device (including "caller ID" units) is permitted only after a court order is obtained, in accordance with Sections 3121-3127 of Title 18, U.S.C.

b. Notice to all users (e.g., 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 (e.g., it would alert a target of the fact of an investigation), a court order must be obtained.

d. Where user consent 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 installing and using a pen register or trap and trace device.

(2) The application must 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.

e. Emergency authorization to use and install a pen register or trap and trace device must be requested in accordance with Section 3125 of Title 18, U.S.C., through coordination with the local U.S. attorney or the DOJ, Office of Enforcement Operations.

3.5. 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 the Judge Advocate General, 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 status-of-forces agreement, or any other agreement with the host country.

b. If the target of the law enforcement investigation is subject to Federal prosecution under the Military Extraterritorial Jurisdiction Act or other possible prosecution in Federal district courts, the investigative DoD Component must consult with the supporting SJA (or other appropriate legal counsel) and the DOJ, Office of International Affairs, to ensure that installing such devices is permitted in accordance with U.S. laws, and does not violate host country laws, any applicable status-of-forces agreement, 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 Military Extraterritorial Jurisdiction Act or other possible prosecution in the Federal district court, the investigative DoD Component must consult with the supporting SJA (or other appropriate legal counsel) and the DOJ, Office of International Affairs, to ensure installing such devices is in accordance with host country laws, any applicable status-of-forces agreement, and any other agreement with the host country.

d. 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 level or higher.

3.6. MOBILE TRACKING DEVICES.

a. A warrant for installing a mobile tracking device may be issued by courts so empowered by law in accordance with Section 3117 of Title 18, U.S.C.

b. Such an order may authorize the use of that device within the court's jurisdiction and outside that jurisdiction if the device is installed in the jurisdiction.

3.7. ACCESS TO, OR RECORDS CONCERNING, ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE OR IN A REMOTE COMPUTING SERVICE.

A DoD Component may obtain access to, and records concerning, electronic communications in electronic storage or in a remote computing service for law enforcement in the United States and its territories in accordance with Section 2703 of Title 18, U.S.C. This does not apply to government-owned and operated computer networks that do not provide services to the public.

a. Electronic Communications Held in Electronic Storage

Access to the contents of an electronic communication held in electronic storage, regardless of the length of time held in such storage, and to non-content location history information as limited by *Carpenter v. United States*, 138 S. Ct. 2206 (2018), is permitted only pursuant to:

(1) A Federal warrant issued in accordance with the Federal Rules of Criminal Procedure by a court of competent jurisdiction,

(2) A State warrant issued in accordance with State warrant procedures; or

(3) For court-martial or other proceeding, in accordance with the UCMJ or regulations prescribed by the President.

b. 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 and non-content location history information as limited by *Carpenter v. United States*, 138 S. Ct. 2206 (2018), covered by Paragraph 3.7.a., may be obtained:

(1) By administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena (limited to basic subscriber information in accordance with Section 2703(c)(2) of Title 18, U.S.C.);

(2) By warrant, as described in Paragraph 3.7.a.;

(3) By court order in accordance with Section 2703(d) of Title 18, U.S.C.; or

(4) With the consent of the subscriber or customer.

c. Prospective Location Records Concerning Electronic Communication Service.

(1) Access to prospective cell-site location information about a subscriber or customer of an electronic communication service in accordance with Section 2703 of Title 18, U.S.C., may be obtained by a warrant issued by a court of competent jurisdiction.

(2) Access to prospective enhanced 911 global positioning system or latitude-longitude data about a subscriber or customer of an electronic communication service in accordance with Section 2703 of Title 18, U.S.C., may be obtained by a warrant as described in Paragraph 3.7.a. The supporting SJA, trial counsel, DOJ trial attorney, or Assistant U.S. Attorney must be consulted to identify the current legal implications and limitations in requesting such process.

SECTION 4: RECORDS

4.1. GENERAL.

All requests for authorizations or denials of recordings and records of information obtained through interception activities accomplished pursuant to this instruction must be retained and safeguarded in the DCIO investigative file in accordance with Chapters 31 and 33 of Title 44, U.S.C.; Parts 1220-1228 of Title 36, Code of Federal Regulations; and DoDI 5015.02.

4.2. REQUIREMENTS.

a. All records pertaining to consensual and nonconsensual interceptions, including denied and unexecuted applications, must be maintained in the permanent investigative case files and will not be destroyed earlier than required by Paragraph 4.1., even if the investigative file may otherwise be destroyed in accordance with DCIO destruction procedures.

b. Recordings of the interceptions made in the United States and its territories pursuant to Section 2518 of Title 18, U.S.C., may be destroyed only upon an order of the court involved. Recordings must be maintained for at least 10 years when not ordered to be destroyed by the court involved.

4.3. DENIED INTERCEPTION APPLICATIONS.

Records of all applications submitted to, and disapproved by, a U.S. District Court or military judge for authorization for a nonconsensual interception of a wire, electronic, or oral communication must be preserved and maintained in the DCIO investigative file and include:

a. 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. City, State, and judicial district of the interception. If known, address(es) of the location or the interception applied for.

d. Case number or other identifier for the application.

e. 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.

4.4. INTERCEPTION APPLICATION APPROVED BUT NOT EXECUTED.

Interception application information must be retained in the DCIO investigative file when an interception was authorized, but not executed.

4.5. RETENTION.

Data must be retained in accordance with the DoD Component's disposition instructions for investigative records as described in Title 36, Code of Federal Regulations.

4.6. DISSEMINATION CONTROLS.

a. All recording and records of information obtained through interception activities pursuant to this instruction must only be used pursuant to Sections 2517 and 2518(1)(e) of Title 18, U.S.C.

b. In all cases, access to information obtained through interception activities in accordance with this instruction must be restricted to only those individuals having a need to know for the proper performance of their official duties in accordance with Section 2517 of Title 18, U.S.C.

c. The information may be disseminated outside the DoD only when:

(1) Authorized by Section 2517(6) of Title 18, U.S.C.

(2) Required by law, including:

(a) Section 552a of Title 5, U.S.C., also known as the "Privacy Act of 1974," as implemented in DoDI 5400.11;

(b) Section 552 of Title 5, U.S.C., also known as the "Freedom of Information Act of 1966"; or

(c) By order of a Federal court.

(3) Requested by a congressional committee.

(4) Required by a status-of-forces agreement or another international agreement.

4.7. RETENTION AND DISPOSITION.

a. The records of a wire, electronic, or oral communication interception not otherwise contained in the permanent criminal investigative file must be retained and disposed of in accordance with the records disposition instructions of the DoD Component concerned.

b. Recordings of the interceptions made in the United States and its territories pursuant to Section 2518 of Title 18, U.S.C., may be destroyed only upon an order of the court involved. Recordings must be maintained for at least 10 years when not ordered to be destroyed by the court involved.

SECTION 5: INTERCEPTION EQUIPMENT

5.1. CONTROL.

The DCIOs must:

a. Establish controls to ensure that only the minimum quantity of interception equipment required to accomplish assigned missions is procured and retained in the DCIO's inventories.

b. Ensure interception equipment is safeguarded to prevent unauthorized access or use and maintain inventory records accounting for all interception equipment at all times.

c. Restrict access to interception equipment and only permit withdrawal and use of such equipment pursuant to DCIO policy.

5.2. DISPOSAL.

a. 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 secretive 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 in accordance with Section 2512(1)(b) of Title 18, U.S.C.

(1) Disposal of interception equipment outside of the Federal Government is prohibited, except as specifically authorized by this instruction.

(2) The DCIO disposing of interception equipment must ensure that the equipment is either transferred to an agency authorized to use it or that the equipment is destroyed.

b. If there are questions about the primary purpose of an item of equipment, the official involved will prohibit its sale pending referral to the Secretary of the Military Department concerned; the IG DoD; or the General Counsel of the Department of Defense. Component general counsel will resolve any legal issues in coordination with the General Counsel of the Department of Defense.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
DCIO	Defense Criminal Investigative Organization
DoDI	DoD instruction
DOJ	Department of Justice
IG DoD	Inspector General of the Department of Defense
SJA	staff judge advocate
UCMJ	Uniform Code of Military Justice
U.S.C.	United States Code

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
consensual interception	Defined in Section 2511(2)(c) and (d) of Title 18, U.S.C.
contents	Defined in Section 2510(8) of Title 18, U.S.C.
counterintelligence	Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities.
court of competent jurisdiction	Defined in Section 3127 of Title 18, U.S.C.
DCIO	Defined in DoDI 5505.03.
DoD personnel	Military Service members and DoD Federal civilian employees hired and paid from appropriated and non-appropriated funds under permanent or temporary appointment.
electronic communication	Defined in Section 2510(12) of Title 18, U.S.C.

TERM	DEFINITION
electronic communication service	Defined in Section 2510(15) of Title 18, U.S.C.
electronic storage	Defined in Section 2510(17) of Title 18, U.S.C.
foreign intelligence	Information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.
intercept	Defined in Section 2510(4) of Title 18, U.S.C.
mobile tracking device	An electronic or mechanical device which permits the tracking of the movement of a person or object.
oral communication	Defined in Section 2510(2) of Title 18, U.S.C.
pen register	Defined in Section 3127(3) of Title 18, U.S.C.
remote computing service	Defined in Section 2711(2) of Title 18, U.S.C.
status-of-forces agreement	A bilateral or multilateral agreement that defines the legal position of a visiting military force deployed in the territory of a friendly state.
trap and trace device	Defined in Section 3127(4) of Title 18, U.S.C.
user	Defined in Section 2510(13) of Title 18, U.S.C.
wire communication	Defined in Section 2510(1) of Title 18, U.S.C.

REFERENCES

Attorney General Memorandum, "Procedures for Lawful, Warrantless Monitoring of Verbal Communications," May 30, 2002[1]

Code of Federal Regulations, Title 36

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Directive 5106.01, "Inspector General of the Department of Defense (IG DoD)," April 20, 2012, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM)," April 3, 2014, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5505.03, "Initiation of Investigations by Defense Criminal Investigative Organizations," August 2, 2023

DoD Instruction 5505.17, "Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities," December 19, 2012, as amended

DoD Instruction 8523.01, "Communications Security," January 6, 2021

DoD Instruction 8560.01, "Communications Security (COMSEC) Monitoring," August 22, 2018

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended[2]

Supreme Court Reporter, "*Carpenter v. United States*," Volume 138, Page 2206 (2018)[3]

United States Code, Title 5

United States Code, Title 10, Chapter 47 (also known as the "Uniform Code of Military Justice (UCMJ)")

United States Code, Title 18

United States Code, Title 44

United States Constitution, Fourth Amendment

[1] Available on the United States Department of Justice website at: https://www.justice.gov/sites/default/files/ag/legacy/2009/02/10/ag-053002.pdf

[2] Available on the National Archives Federal Register website at: https://www.federalregister.gov/d/E8-17940

[3] Will be included in Volume 585, U.S. Reports for 2018 (585 U.S. ____ (2018)) when published.