



TECHNICAL OPERATIONS GROUP

15.1 Technical Operations Group

SPECIAL SERVICES AND THE NATURE OF TECHNICAL OPERATIONS

Technical Operations includes electronic surveillance, technical surveillance countermeasures, aerial surveillance, and wireless communications. TOG maintains a variety of special equipment and capabilities—some of which may fall outside the traditional definition of “technical” or “electronic” devices. Investigators are encouraged to visit the TOC or R/TOCs and to consult with the ESU inspectors responsible to their region regarding these capabilities. TOG is continuously working to meet the challenge of both new and obsolete technologies and law to provide premier investigative technical support to the USMS and to other federal, state, and local government agencies.

A. General

1. **TOG Structure:** The Investigative Operations Division's Technical Operations Group (TOG) provides technical equipment and support to the United States Marshals Service (USMS) and other federal, state, and local government agencies. TOG is a headquarters element and is commanded by a Chief located at the Technical Operations Center (TOC). There are multiple Regional Technical Operations Centers (R/TOCs) headed by Chief Inspectors. The R/TOCs consist of Electronic Surveillance Unit (ESU) inspectors and equipment; Technical Surveillance Countermeasures (TSCM) inspectors and equipment; Air Surveillance Operations (ASO) pilot-inspectors and aircraft; and Operational Wireless Communications Support (OWCS) inspectors and transportable command & control equipment. The R/TOCs may further deploy inspectors to various cities within their regions. For purposes of this policy, ESU, TSCM, ASO, OWCS inspectors are identified as “TOG inspectors.” The general structure of TOG is identified below:

**Investigative Operations
Division (IOD)**
Assistant Director
Inspectors & Staff
(Other operations omitted
here)

**Technical Operations Group
(TOG)**
Chief, TOG
Inspectors & Staff

**Electronic
Surveillance Unit
(ESU)**
Chief Inspectors
(R/TOCs)

**Technical
Surveillance
Countermeasures
(TSCM)**
Inspectors

**Air Surveillance
Operations (ASO)**
Chief Pilot
&
Pilot-Inspectors

**Operational Wireless
Communications
Support
(OWCS)**
Chief Inspector

Technical Operations Group Topics

Inspectors & Staff (R/TOCs & Cities)	Inspectors (Cities)	Inspectors (R/TOCs)	& Inspectors/Staff (R/TOCs)
---	------------------------	------------------------	-----------------------------------

a **ESU:** The Electronic Surveillance Unit (ESU) provides trained surveillance investigators and specialized equipment for investigative support and training. This includes electronic intercept, audio and video surveillance and monitoring, physical and electronic tracking, and computer forensic analysis and intercept. ESU is the primary investigative support unit of TOG. Requests for ESU support should be routed through an ESU inspector.

b **TSCM:** Technical Surveillance Countermeasures (TSCM) inspectors provide equipment and expertise in the conduct of surveys for the detection of technical surveillance penetrations in situations which appear to be hostile surveillance efforts, or where hostile exploitation of fortuitous circumstances is indicated. TOG inspectors will also provide guidance to USMS personnel with regard to exploitable technical situations which are not the result of deliberate hostile surveillance efforts. Requests for TSCM support should

b2/7E

c. **ASO:** Air Surveillance Operations (ASO) provides aerial support to ESU and other USMS components for operational support. Requests for ASO support that do not also include ESU support should be routed through an ASO Pilot-Inspector.

d. **OWCS:** Operational Wireless Communications Support (OWCS) is the USMS representative to the Department of Justice (DOJ) initiative to more fully utilize and consolidate emergent communications technologies. The OWCS oversees the USMS radio, microwave, and satellite communications program and makes agency-wide acquisition and deployment determinations. The OWCS maintains highly specialized communications equipment that is available to districts, task forces and headquarters elements for emergency-response command centers and disaster coordination, special events, high-threat enforcement operations and trials, and similar large-scale events. Investigative requests for OWCS support (i.e. other than routine radio issues) that do not also include ESU support should be routed through an OWCS inspector.

2. **TOG Internal Procedures:** Because much of TOG's capabilities, methods and resources are classified or are otherwise "Law Enforcement Sensitive", this section sets forth only general guidelines, policies and procedures governing TOG's function and role within the USMS. The Chief, TOG is charged with implementing TOG's internal operating procedures consistent with federal law and National Security and Intelligence directives and initiatives. Those aspects of TOG's internal operating procedures that are reduced to writing or other recorded format shall be properly marked and safeguarded and shall not be disseminated outside TOG without the express written approval of the Chief, TOG or his authorized superior.

3. **TOG Capabilities:** USMS districts, task forces and headquarters elements shall follow these guidelines when requesting TOG assistance or utilizing ESU equipment. Investigators are encouraged to consult frequently with TOG inspectors regarding new capabilities and available resources. To the extent that investigators acquire knowledge of sensitive or classified information or programs incident to their investigation or consultation with TOG, they shall safeguard that information and shall not divulge it outside the USMS without express written approval from the Chief, TOG or his designated representative—unless otherwise directed by a court of competent jurisdiction.

4.

b2/7E

Technical Operations Group Topics

TECHNICAL EQUIPMENT PROCUREMENT AND USE

- A. **TOG-Only Equipment:** Subject to the exceptions identified below, no USMS district, task force or headquarters element may purchase or maintain the following types of equipment or software without the express approval of the Chief, TOG or his designated representative.
1. Equipment or software designed or readily capable of surreptitiously intercepting another's telephone or wireless voice communications or their dialed or digital identifiers.
 2. Equipment or software designed or readily capable of intercepting or recording another's electronic correspondence, data communication, internet or network activity, keystrokes, file access or use, video-monitor display, user identification or password.
 3. Equipment designed to be clandestinely placed to surreptitiously monitor or record audio or video (e.g. hidden or disguised audio or video transmitters, miniature cameras or microphones, and wire transmitters designed to be worn by an undercover agent or source).
 4. Equipment designed to electronically enhance live audio or video (e.g. parabolic microphones or thermal imaging equipment).
 5. Technical Surveillance Countermeasure Equipment (TSCM) or equipment designed to detect the presence of clandestinely placed monitoring equipment.

Because technology and capabilities are numerous and evolving, the list above is illustrative rather than exhaustive. To assure compliance with federal law, DOJ directives, and to avoid acquiring duplicate resources, districts, task forces and headquarters elements shall consult with ESU prior to acquiring technology or equipment designed to electronically monitor or intercept another's activities.

B. Exceptions

1. Districts, task forces, and headquarters elements may use and purchase video and audio equipment used primarily for security purposes, interviews, prisoner monitoring, consensual phone monitoring, and day or night surveillance equipment that magnifies or enhances ambient or infrared light (e.g. binoculars and night-vision goggles).
2. For administrative purposes, the Information Technology Division (ITD) branch of the may monitor routine network activity and communications sent or received using government resources to assure network availability and compliance with DOJ/USMS policy and ethics guidelines. Criminal investigations and computer forensic analysis shall be conducted by TOG personnel or those designated by the Chief, TOG.
3. The Judicial Security Division (JSD) may maintain TSCM equipment for use by TSCM-trained investigators.
4. USMS investigators may participate on task forces that purchase or maintain the foregoing equipment using non-USMS funds.

MAINTAINING AND USING TOG EQUIPMENT

TOG inspectors may loan certain items of unclassified or non-sensitive electronic surveillance or communications equipment to districts, task forces, or headquarters elements for use by appropriately trained and experienced investigators without the presence of a TOG inspector. Loaned equipment shall be stored in climate-controlled and secure government storage locations approved of in advance by a TOG inspector. Loaned equipment may not be left unattended in locked vehicles unless its operational use is imminent. ESU equipment shall be hand-carried between USMS personnel or shipped via an insured carrier that tracks and receipts its shipments. In cases where damage or loss is caused to loaned equipment owing to intentional or negligent misuse or storage, the district, task force or headquarters element shall bear the cost of repairing or replacing the item.

REQUESTING TOG SUPPORT

Technical Operations Group Topics

- A. **How to Request:** Requests for TOG support shall be submitted through ESU on form USM-11 at the earliest time permitted by an investigation. Prior to submitting a USM-11 or obtaining a court order or subpoena, investigators shall discuss their operation with a TOG inspector to assure the sufficiency of the proposed order, subpoena or request and the availability of TOG resources to meet the specific investigative objective. TOG inspectors maintain a variety of "go-by" court orders that investigators may adapt to their specific case. The U.S. Attorneys' Offices (USAO) will have district-specific orders, the language of which has been previously approved by their judges.
- B. **Authority to Request:** Many of TOG's operations require additional funding and/or payment to third parties. Thus, investigators and inspectors should work together to assure that TOG assets are deployed where most likely to positively impact the success of major activities. District and task force investigators must apprise their supervisor of their request for TOG support prior to its submission. Implicit with a submitted request for assistance is a district or task force management's approval; and form USM-11s should reflect supervisory approval. No electronic intercept court orders may be sought without prior approval from a TOG inspector.
- C. **Exigencies:** Rapidly evolving investigations and events impacting community or officer safety may preclude an investigator from obtaining a court order or subpoena prior to requiring TOG support. In such cases, the consulting TOG inspector shall evaluate the case and determine whether or not the facts amount to "exigent circumstances" sufficient to warrant immediate monitoring. In all cases where a court order or subpoena is required and TOG has initiated "exigent circumstances" monitoring, the requesting investigator shall, within 48 hours (weekend, holiday or otherwise) of the initiation of monitoring, submit the supporting court order or subpoena for judicial, grand jury, or administrative approval. In the event a court order or subpoena is denied or otherwise unavailable, the investigator will immediately notify the consulting TOG inspector, who will either cease monitoring or assist the investigator and prosecutor in expeditiously submitting a revised order or subpoena.

WHEN TOG SUPPORT MUST BE REQUESTED

- A. TOG inspectors and their superiors are the only USMS personnel who may conduct or otherwise authorize the following categories of technical investigation, regardless of whether the USMS or another investigative agency ultimately provides technical support:
1. Electronic voice intercept or monitoring (e.g. body wires and listening devices)
 2. Non-consensual telephone intercept or monitoring (including wireline, wireless, cable, facsimile, or internet telephone voice communication), but excluding all consensual telephone and non-telephonic radio monitoring.
 3. Pager or two-way message intercept or monitoring, including numeric, text or voice messages and non-voice data sent to or from any wireless device.
 4. Computer or electronic data intercept, monitoring, "hacking," or forensic analysis for criminal investigative purposes.
 5. Telephone call analysis, monitoring, or intercept using pen registers/remote dialed number recorders, non-consensual trap and traces, or wireless telephone tracking (including live signal intercept or historical cell-site or tower data).
 6. Electronic tracking utilizing devices that direction-find, location-transmit or location-store (e.g. bird dogs and tele-trackers).
 7. Video surveillance for investigative purposes using specialized cameras that are disguised, hidden, miniature, thermal imaging, or wirelessly transmit images or data.
 8. Signals intercept using equipment that is designed or capable of intercepting encoded, encrypted or digital wireless or communications signals.
 9. Signals intercept using equipment that is designed or capable of receiving electronic emissions from video monitors or other electronic devices not specifically mentioned above.
 10. Surreptitious entry into buildings, vehicles and containers.

Technical Operations Group Topics

SECURITY AND PROTECTION

- A. **Physical Security:** During ESU installations and operations, TOG inspectors are acting in an undercover capacity and may modify their physical appearance or identity to suit the investigative mission. In order to protect themselves and maintain the integrity of the investigation, TOG inspectors may be required to perform their tasks going unnoticed by the subject of the investigation and his associates, telephone and utility carriers, and local law enforcement authorities. Wherever possible, two TOG inspectors will complete high-profile or otherwise high-risk installations of specialized equipment. When circumstances require, the requesting district, task force or headquarters element shall ensure that adequate back-up and security is available to TOG inspectors.
- B. **Protecting TOG Techniques:** All investigators involved in utilizing TOG equipment, software or methods in the course of their investigation should be aware that the compromise of those techniques may later become necessary to the production of evidence and successful prosecution at trial. It is imperative that investigators understand that they must minimize, to the greatest extent legally possible, any testimony by TOG personnel or the disclosure of TOG techniques throughout the judicial process. Disclosures could reveal investigatory records compiled for electronic surveillance support purposes, specialized techniques utilized by TOG, or the location, capabilities and frequencies of electronic equipment. Such disclosure could significantly impair the future effectiveness of the technique and jeopardize the safety of ongoing and future surveillance operations by both the USMS and other investigative agencies. Any investigator involved in trial preparation in which TOG techniques were employed shall immediately contact their TOG inspector for guidance. There is case law addressing investigative privilege to protect these techniques and the Office of General Counsel and ESU will assist in protecting this information.

LEGAL OVERVIEW

The law with respect to electronic intercept and monitoring as it relates to criminal investigations is still in its infancy and is rapidly evolving. Certain provisions of the following Acts have shaped the landscape of electronic surveillance law.

- A. **OCCSSA:** The principal and most important electronic intercept laws were first passed under Title III of the Omnibus Crime Control and Safe Streets Act (OCCSSA) of 1968. The OCCSSA's electronic intercept provisions are divided and codified into (i) the "wiretap" chapter at 18 USC 2510-2522, used primarily for intercepting live, content-based communications (and generally known as "Title III"), and (ii) the Pen Register and Trap and Trace Device chapter (distinguished as "the Pen/Trap Statute", despite the fact that it was also created under the same title) at 18 USC 3121-3127, used primarily for intercepting live, non-content based transactional records and data. Failure to comply with these statutes may result in the suppression of evidence and civil and criminal liability. Not Correct Statutorily
- B. **Cable Act:** The Cable Communication Policy Act of 1984 ("Cable Act"), principally at 47 USC 521 et seq., affords privacy protection to cable subscribers and limits the circumstances concerning the release of personally identifying information. Specifically, law enforcement must obtain a court order based upon clear and convincing evidence that the cable subscriber is engaged in criminal activity and that the information sought is material to the case. In addition, the cable subscriber whose information is sought must be afforded the opportunity to contest the disclosure at a hearing before disclosure occurs. Once cable companies began providing telephone and internet service, the advance-notice provisions of this chapter became investigatively untenable.
- C. **ECPA:** The Electronic Communications Privacy Act ("ECPA") of 1986, principally at chapter 121, 18 USC 2701-12, governs how investigators can obtain stored communications content and non-content transactional records and data from telephone companies, wireless/cellular telephone service providers, network service providers, including Internet service providers (ISPs), and satellite services. Increasingly, ECPA issues arise in cases involving the internet: any time investigators seek stored information concerning Internet accounts from providers of Internet service, they must comply with the statute. ECPA also made comprehensive revisions to Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and clarified the legal requirements regarding law enforcement investigative techniques in light of the technological advances in the area telecommunications and computers.
- D. **CALEA:** The Communications Assistance for Law Enforcement Act (CALEA) of 1994 was established to provide parameters within which information and communications transmitted in technologically advanced and sophisticated methods may be accessed by law enforcement. The Act defines the responsibilities of

Technical Operations Group Topics

- telecommunications carriers to provide access pursuant to court order or other lawful process and authorizes the Attorney General to expend \$500 million to assist carriers in making the necessary technical modifications to their facilities and services to ensure law enforcement access and uniform data formatting. The Act also (i) specified that radio communications between a cordless telephone handset and base are protected under Title III, (ii) defined terminology consistent with technological advances, (iii) required carriers to pass along call-identifying data, and (iv) provided an enforcement mechanism to compel service providers to comply with Title III wiretap orders.
- E. **Antiterrorism Act:** The Antiterrorism and Effective Death Penalty Act of 1996 modified the definition of "electronic communication" to exclude information stored in a communications system used for the electronic storage and funds transfers, and clarified which radio communications are legally considered to be "readily accessible to the general public."
- F. **The Patriot Act and Its Sunset:** Following the September 11, 2001 terrorist attacks, Congress quickly enacted the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act ("PATRIOT" Act) of 2001—a broad set of emergency laws designed to remove many of the impediments faced by the law enforcement and intelligence communities in their efforts to fight terrorist activities and share information. Many of the provisions of the PATRIOT Act directly impact criminal investigators' use of Title III, the Pen/Trap Statute, and ECPA. Unless re-enacted into law, many of these provisions sunset (revert) on December 31, 2005—and the advances made by the PATRIOT Act will be lost. Accordingly, investigators are urged to inform TOG whenever use of the new authorities proves helpful in a criminal case. This information will help ensure that Congress is fully informed when deciding whether to re-enact these provisions. Significant PATRIOT Act changes include:
1. **Stored Communications:** Sections 209, 210, 212 and 220 amend 18 USC 2702 and 2703 by (i) including stored wire communications, thereby eliminating the necessity of obtaining a Title III order to access voice-mail, (ii) expanding the list of information available pursuant to subpoena, (iii) permitting voluntary disclosure of records when necessary for a provider to protect itself and for law enforcement emergencies, and (iv) providing nationwide effect for electronic correspondence (email) search warrants.
 2. **Cable Act:** Section 211 amends the Cable Act at 47 USC 551(c)(2)(D) to clarify that ECPA, Title III, and the Pen/Trap statute govern disclosures by cable companies that relate to the provision of communication services (e.g. telephone and Internet services). The amendment preserves, however, the Cable Act's heightened protection of records revealing what ordinary cable television programming a customer chooses subscribes to or purchases. This section is not subject to the Act's sunset provision.
 3. **PEN/TRAP:** Section 216 modifies 18 USC 3121, 3123, 3124, and 3127 to recognize new technologies and the application of pen/traps to those technologies, such as internet activity. The modification also gives nationwide effect to pen/trap orders and requires court oversight when the government installs a pen/trap without a provider's assistance.
 4. **TITLE III:** Section 217 modifies 18 USC 2511 to allow computer trespassing victims (e.g. service providers or hacking victims) to pro-actively collect data and seek law enforcement assistance to monitor any information transmitted to, through, or from a protected computer (but excluding authorized but non-consenting users' information).
 5. **Intelligence Community:** Sections 504, 505, and 901-907 modify the Foreign Intelligence Surveillance Act (FISA) of 1978 and the National Security Act of 1947 by recognizing the need for and authorizing law enforcement and the intelligence community to share information lawfully obtained pursuant to criminal and intelligence investigative efforts as it relates to terrorist activities or funding and foreign intelligence or attack.
- G. **The Homeland Security Act of 2002:** The Cyber Security Enhancement Act, appearing as section 225 of the Homeland Security Act of 2002, (i) increased the penalties for illegal privacy-interest invasions (computer hacking, monitoring wireless telephone communications, accessing stored communications, and advertising or selling illegal interception devices) (ii) loosened the circumstances under which internet service providers may voluntarily disclose inadvertent discovery of communications content to authorities; and, (iii) expanded pen/trap authority to include immediate threats to national security and ongoing attacks on protected computers.
- H. **Departmental Restrictions:** The Attorney General has further restricted some types of monitoring

Technical Operations Group Topics

practices, requiring agency approval from the Department of Justice (DOJ) Office of Enforcement Operations (OEO) or higher authority, and imposing various reporting requirements. Those restrictions are identified below with their corresponding category of monitoring.

- I. **Future Legislation and Departmental Policy:** Investigators can expect the landscape of electronic surveillance law to continue to change in exponential manner. As investigators discover legal obstacles and new technologies not adequately addressed by existing law, they should submit the facts and circumstances surrounding the investigation and their objective and describe the particular challenge. TOG maintains close contact with investigative, intelligence and legislative leaders and with the DOJ OEO attorneys responsible for submitting proposed statutory modifications to Congress.
- J. **Consultation With TOG:** Because the law and Departmental Policy with respect to electronic surveillance is rapidly evolving and is constantly subject to change, prior to engaging in any type of electronic surveillance (whether or not TOG's technical assistance or equipment is required under this policy) or consulting with the USAO regarding proposed court orders, investigators shall consult with a TOG inspector to ensure that they are complying with current law, collection practices, and authorization and reporting requirements—in addition to verifying that the proposed intercept is technically possible and financially warranted. As with technical capabilities, the legal authority and restrictions discussed herein are by no means exhaustive. TOG inspectors and their legal counsel are best suited to make determinations regarding the legality and propriety of any proposed intercept.



TECHNICAL OPERATIONS GROUP

15.1 Technical Operations Group

USMS MONITORING OPERATIONS AND COMMUNICATIONS CATEGORIES

- A. Who May Authorize and Conduct Monitoring Within the USMS:** With the general exception of (i) consensual telephone intercept where the investigator is physically present with the consenting party, and (ii) radio frequency intercept that does not occur between a telephone handset and base:
1. Only TOG inspectors and their superiors may authorize consensual monitoring of communications. Once properly authorized and logged, investigators may monitor without a TOG inspector's supervision.
 2. Only TOG Chief Inspectors or their superiors may authorize non-consensual monitoring operations pursuant to Title III or the Pen/Trap Statute. Once properly authorized and logged, all such monitoring must be supervised by a TOG inspector.
- B. Communications Categories:** Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC 2510-2522), as amended by the Electronic Communications Privacy Act (ECPA) of 1986, the Communications Assistance for Law Enforcement Act (CALEA) of 1994, the Antiterrorism and Effective Death Penalty Act (Antiterrorism Act) of 1996, and the USA-PATRIOT Act of 2001 are referred to collectively as "Title III" to the extent they pertain to intercepting communicative content. When uttered or transmitted where there exists a reasonable expectation of privacy, non-consensual oral, wire and electronic communications intercepts must be made pursuant to a Title III court order. For purposes of Title III, a communication includes the informational content that is intentionally uttered or transmitted, but does not include certain stored communications or non-content transactional records and data incidentally associated with the communication.
1. **Oral Communications:** Oral communications are "aural transfers" (involving the human voice) that are NOT transmitted by wire. "Oral communications" are only treated as such by Title III when they involve utterances by a person possessing a reasonable expectation of privacy, such as conversations within a person's residence, private office, or car. 18 USC 2510(2).
 2. **Wire Communications:** Wire communications are "aural transfers" (involving the human voice) that are transmitted, at least in part by wire, between the point of origin and the point of reception (18 USC 2510(1)). This includes voice communications conducted over wireless telephones, cordless telephones, traditional telephones, and voice pagers—all of which require wire at some point to transmit their communications.
 3. **Electronic Communications:** An "electronic communication" is one in which the human voice is not used in any part of the communication. 18 USC 2510(12). Title III electronic communications applications are most commonly utilized for digital-display pagers, electronic facsimile machines and email, internet or file transfer. Applications for these types of interceptions must comply with the requirements set forth in 18 USC 2518.
 4. **Radio/Microwave/Satellite Communications:** Radio, microwave and satellite communications are generally not protected under Title III unless they are also wire (e.g. telephonic in nature) communications or are not "readily accessible to the general public." 18 USC 2511(g).

WARRANTLESS MONITORING

- A. Consensual Oral Monitoring that Requires Approval:** By Attorney General memorandum dated May 30, 2002, warrantless consensual oral monitoring (usually accomplished by a body-wire transmitter or other fixed

Technical Operations Group Topics

listening device when there is at least one consenting person present at all times) requires both (i) agency approval from a high-ranking supervisory official at headquarters level, and (ii) advice from the U.S. Attorney or Assistant U.S. Attorney (AUSA or other DOJ attorney responsible for the investigation) that the proposed monitoring is both legal and appropriate. The approval and logging requirements of this section apply to consensual oral monitoring that is conducted electronically, mechanically or by other device—but DO NOT apply to consensual wire (telephone) monitoring or radio monitoring, or the four additional monitoring exceptions listed below.

B. Oral Monitoring Investigations that Require Written Departmental Approval: In addition to securing agency and AUSA approval to conduct a consensual monitor, the Attorney General's May 30, 2002 Memorandum designated six (6) categories of warrantless oral monitoring, consensual or otherwise, that require written Departmental approval. In all such cases, investigators should consult with a TOG inspector, who will route the request through appropriate channels to the Director or Associate Director of DOJ OEO for approval. These categories are:

1. **Senior U.S. Officials:** Monitoring relates to an investigation of a member of Congress, a federal judge, or a member of the Executive Branch at Level IV or higher, or a person who has served in such capacity within the previous two years.
2. **Senior State Officials:** 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. **Diplomats:** Monitoring where any party to the communication is a member of the diplomatic corps of a foreign country.
4. **Protected Witnesses:** Monitoring where 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. **Federal Prisoners:** Monitoring where any party to the communication is in the custody of the Bureau of Prisons (BOP) or the USMS.
6. **Upon Request:** Any case in which the Attorney General, his deputy, associate or assistant, 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.

C. When Approval is not Required: Even if the investigation falls into one of the foregoing six categories, no additional Department approval or logging is required for the following monitoring:

1. Extraterritorial intercept.
2. Foreign intelligence intercept, including intercept pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 USC 1801 et seq.)
3. Intercept pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 USC 2510 et seq.)
4. Routine Bureau of Prisons monitoring of oral communications not attended by a justifiable expectation of privacy.
5. Intercept of non-telephonic radio communications.
6. Intercept of consensual telephone communications.

D. USMS Approval Authority: Consistent with Departmental directive, the Director, Deputy Director, Assistant Director for Investigations, and Chief, TOG (and his designated Chief Inspectors) are the only USMS personnel who may authorize the foregoing types of warrantless consensual monitoring for investigative purposes. In most cases, investigators should receive oral or written AUSA advice prior to seeking approval through a TOG inspector. If the AUSA consulted cannot give advice for reasons unrelated to the legality or propriety of monitoring, the TOG inspector will route the request through appropriate channels to the designated DOJ Criminal Division attorney for approval.

Technical Operations Group Topics

- E. Monitoring Log:** DOJ agencies must maintain a warrantless consensual oral monitoring log that includes: (1) the reason for monitoring, (2) the offense being investigated and its statutory citation, (3) the danger faced by a consenting party if the monitoring is for protection, (4) the location of the device, whether on a person, personal effects, or fixed, (5) the location and primary judicial district where monitoring is to occur, (6) the time needed for the monitor (up to 90 days per request, with additional 90 day extensions), (7) the names of the persons expected to be monitored and their relation to the investigation, (8) the attorney whose advice was sought and the date on which advice was provided, and (9) the renewal status, investigation status, and a reference to all prior authorizations and the fact that attorney advice was again obtained for each renewal. The Chief, TOG will maintain the monitoring log for the USMS and shall provide it to the Department upon request.
- F. Custodial Monitoring and DOJ Restrictions:** Generally, detainees and prisoners have no reasonable expectation of privacy. Although the courts have upheld warrantless monitoring of a prisoner's telephone conversations under theories of both consent and the "law enforcement exception," occasionally the courts have held that neither exception applies. In 1987, the Department's Criminal Division established guidelines for the Bureau of Prisons (BOP) on law enforcement access to electronically monitored and intercepted inmate telephone calls. These guidelines require law enforcement to obtain a court order or a subpoena to obtain inmate telephone calls in connection with a criminal investigation.
1. **BOP-Initiated Disclosure:** BOP may voluntarily disclose routinely monitored inmate telephone conversations if the conversation is found to contain information relating to the violation of federal or state law.
 2. **Investigative Requests for Recorded Communications:** A grand jury subpoena or other process is required when outside law enforcement agencies request BOP to disclose transcripts of previously monitored general telephone conversations if that request is made in connection with a criminal investigation being conducted of activities outside the confines of the prison regarding specified individuals.
 3. **Investigative Requests for Live Intercept:** A Title III court order is required when outside law enforcement agencies request BOP to monitor and disclose future telephone conversations of specified inmates in connection with a criminal investigation being conducted outside the confines of the prison and not affecting prison security or administration.
- G. Oral Monitoring Exigencies:** Because USMS investigations are often fluid and rapidly developing, prior AUSA or Departmental approval may not be practicable in all cases.
1. **Departmental Approval Required:** For all emergency consensual monitoring cases where written Departmental approval is required, prior approval must be obtained through a TOG Chief Inspector or his superiors, who will seek verbal approval from the Director or Associate Director of DOJ OEO, the Assistant AG, or Deputy Assistant AG for the Criminal Division. In the event verbal Departmental approval cannot be obtained beforehand, the Chief, TOG or his superior may provide verbal approval with follow-up to the Department within three workdays.
 2. **Departmental Approval not Required:** For all emergency consensual monitoring cases where agency approval and attorney advice is required but written Departmental approval is not required, a TOG inspector, supervisory investigator, or deputy-in-charge may verbally approve the request. In such cases, the investigator must consult with an AUSA at the earliest practicable time and shall notify a TOG inspector in writing if approval was granted by other-than TOG personnel.

STORED ELECTRONIC COMMUNICATIONS AND SUBSCRIBER RECORDS

The 1986 ECPA defined and regulated government access to various "new" forms of electronic communications, including stored electronic communications, transactional records and subscriber records. ECPA was clarified and modified by the 2001 USA PATRIOT ACT.

A. Definitions

1. **Electronic Storage:** Electronic storage is any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such

Technical Operations Group Topics

communication. 18 USC 2510(17).

2. **Electronic Communications System:** An electronic communications system includes any entity that provides its users the ability to send or receive wire or electronic communications." S. Rep. No. 541, 99th Cong., 2d Sess. 14 (1986). (e.g. wireless telephone companies and internet service providers)
 3. **Remote Computing Service:** A remote computer services allow persons to use the facilities of these services to process and store their own data. H. Rep. No. 647, 99th Cong., 2d Sess. 23 (1986). (e.g. leaving email messages on a commercial internet service provider's server or utilizing online storage for communicative records or files).
- B. Accessing Communications Stored Within the Last 180 Days:** Only pursuant to a search warrant (based upon probable cause) can the government require a service provider to disclose the contents of an electronic or wire communication that is in electronic storage in an electronic communications system for one hundred and eighty days or less. 18 USC 2703(a)
- C. Accessing Communications Stored More Than 180 Days Ago:** If the contents of the electronic or wire communication have been in electronic storage for more than one hundred and eighty days, disclosure may be required by a search warrant (without prior notice to the subscriber), a court order (with prior notice to the subscriber), or an administrative, grand jury or trial subpoena (with prior notice to the subscriber). 18 USC 2703(b),(d).
- D. Delaying Notice:** The government may seek an order delaying notice to the subscriber of its collection of stored electronic or wire communications for 90 days, with successive applications for 90-day extensions. 18 USC 2705.
- E. Subscriber Records That Providers Must Disclose**
1. **Pursuant To Court Order or Consent:** To the extent specified by the search warrant, court order or consent, an electronic communication service or remote computing service must disclose to a government entity all records pertaining to its subscriber or customer. 18 USC 2703(c)(1).
 2. **Pursuant to Subpoena:** Pursuant to administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena, an electronic communication service or remote computing service may be required to disclose the name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an. 18 USC 2703(c)(2).
 3. **Exigent Circumstances:** Although service providers are not legally required to disclose subscriber records or stored communications content absent legal process, the statute allows them to voluntarily disclose the records if the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay." 18 USC 2702. Most providers will provide such information on an emergency basis provided it is followed-up with the proper legal process and, in some cases, an exigent/emergency request certification. Although 18 USC 2707 protects service providers from civil liability for the "good faith" disclosure of such records, it may not protect them from civil liability for failing to disclose the records to law enforcement in a certified emergency—if that failure results in injury to a third party.
 4. **Notice Not Required:** When the government requests and receives subscriber records that do not include the content of stored electronic or wire communications, there is no subscriber notice requirement. 18 USC 2703(c)(3).
- F. Legal Standard:** The government must offer "specific and articulable facts showing that there are reasonable grounds to believe that...the records or other information sought are relevant and material to an ongoing criminal investigation" when it seeks access to electronic or wire communications stored for more than 180 days through means other than search warrant. 18 USC 2703(d). Search warrants must be based upon probable cause. Fed. R. Crim. P 41.
- G. Preservation Letters:** A service provider or remote computing service, upon request of a governmental

Technical Operations Group Topics

entity, must preserve records and other evidence in its possession for 90 days (and subject to 90-day renewals) pending the issuance of legal process. 18 USC 2703(f).

H. Payment To Providers: The person or entity assembling or providing stored records or communications is entitled to reimbursement for costs "reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing" the records or communications, to include "any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which [the] information [was] stored." 18 USC 2706(a).

1. **Amount of Reimbursement:** The amount of reimbursement "shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production[.]" 18 USC 2706(b).

2. **No Reimbursement for Routine Subscriber or Toll Records:** Providers are not entitled to reimbursement for assembling or providing "records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under 18 USC 2703. Providers may, however, petition the court for reimbursement if the requested information is "unusually voluminous in nature or otherwise caused an undue burden on the provider." 18 USC 2706(c).

I. Requests That Investigators May Make Directly to Providers: Investigators may serve administrative, grand jury or trial subpoenas for subscriber information and ordinary toll records directly upon the service provider. All court orders, exigent circumstances requests, communicative content search warrants or subpoenas, or unusual stored records requests and searches (e.g. calls to destination, verbatim, switch activity searches, etc.) must be made through a TOG inspector. The USMS is charged a fee for certain records searches and only TOG inspectors are authorized to make commitments for such expenditures.

NON-CONTENT INTERCEPT UNDER THE PEN/TRAP STATUTE

Pen register and trap and trace devices may obtain any non-content information (e.g. all dialing, routing, addressing, and signaling information) utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body/text of an e-mail.

A. Definitions

1. **Pen Register:** A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business." 18 USC 3127(3).

2. **Trap & Trace:** A "trap and trace" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 USC 3127(4).

B. Monitoring Prohibited Without Court Order: Except as provided in 18 USC 3121, no person may install or use a pen register or a trap and trace device without first obtaining a court order under 18 USC 3123 or under the Foreign Intelligence Surveillance Act (50 USC 1801, et seq.).

C. Application: The application may be made by an attorney for the government or a state law enforcement or investigative officer, and must certify that the information likely to be obtained is relevant to an ongoing criminal investigation. Unlike Title III pleadings, a pen register application need not establish probable cause and does not require prior Department approval.

Technical Operations Group Topics

- D. Order:** The order, which is valid for sixty days (and may be extended for additional sixty-day periods), must specify the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; the identity, if known, of the person who is the subject of the criminal investigation; the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection 3123(a)(2)(State court order), the geographic limits of the order; the offense(s) to which the information to be obtained from the pen register or trap and trace will relate; and direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device. The order should also direct that the application and order be sealed until otherwise ordered by the court, and that no disclosure of the existence of the pen register or trap and trace or the existence of the investigation be made to the subscriber or other persons until directed by the court. A pen register/trap and trace order is executable anywhere within the United States and, upon service, the order applies to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served. 18 USC 3123(a).
- E. Creating a Combination Order to Include Stored Records:** Investigators should draft their pen/trap application and order to require service providers to also disclose (i) subscriber records and toll records for the pen/trap target and any other connections (e.g. telephone numbers, email recipients, etc.) identified by the pen register or trap and trace device; and, (ii) all wireless tower/cell-site locations and facings being utilized by the target cellular telephone, two-way pager or similar wireless device. Adding the section 2703(d) disclosures will alleviate the burdensome necessity of returning to the court (or obtaining a subpoena) to identify each subsequently identified originating or terminating subscriber; and, more importantly, allows service providers to disclose location-identifying information otherwise prohibited from disclosure by 47 USC 1002(a)(2)(B). (Location identifying information may not be "acquired solely pursuant to the authority for pen registers and trap and trace devices")
- F. Minimizing "Over-Collection" Of Content:** Section 3121(c) requires that a government agency authorized to install and use a pen register or trap and trace device use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. By June 3, 2002 Deputy Attorney General Memorandum, it is Departmental policy that any "over-collection" of content not be used for any affirmative investigative purpose, except to prevent the immediate danger of death, serious physical injury, or harm to national security.
- G. Enforcement of Orders:** The PATRIOT Act modified the Pen/Trap statute so that a federal Pen/Trap court order "shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order"; and that "[w]henver such an order is served on any person or entity not specifically named in the order, upon request...the law enforcement or investigative officer...shall provide written or electronic certification that the order applies to the person or entity being served." 18 USC 3123(a)(1).
- 1. Drafting Orders to Cover Other Providers:** Investigators should draft court orders directing each known service provider and "any other involved person, entity, telecommunications provider or its reseller or agent," to provide the requested assistance and/or records.
 - 2. Civil Penalty for Providers' Non-Compliance:** Failure to provide the information or assistance required by the order is punishable by fine of \$10,000 per day, per violation. 18 USC 2134(f) (incorporating 18 USC 2522, as applicable to Communications Intercept).
 - 3. Stored Records:** Chapter 121, Stored Electronic Communications & Records, of Title 18 contains no provision for the enforcement of orders. Although compelling compliance with a Pen/Trap order that also requires disclosure of stored records (e.g. subscriber) is unclear under this section, investigators should assert that compliance with the entire order is mandatory irrespective of whether a provider is specifically named in the order.
- H. Exigencies:** 18 USC 3125 permits the AG, the DAG, the Assoc. AG, any AAG, any Acting AAG, or any DAAG, or State Attorneys General, to specially designate any investigative or law enforcement officer to

Technical Operations Group Topics

determine whether an emergency situation exists requiring the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained. An emergency situation under this section exists if it involves the immediate danger involving (i) the death or serious injury to any person, (ii) conspiratorial activities characteristic of organized crime, (iii) threats to national security, and (iv) ongoing attacks on protected computers. The government has forty-eight hours after the installation has occurred to obtain a court order in accordance with section 3123 approving the installation or use of the pen register/trap and trace device. Failure to seek a court order within this forty-eight-hour period constitutes a violation of the pen register/trap and trace chapter.

- I. **Payment to Providers:** A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance. 18 USC 3124(c).

MONITORING THE CONTENT OF COMMUNICATIONS UNDER TITLE III

Monitoring or otherwise intercepting non-stored communicative content is the most highly protected individual privacy right in the United States. By statute, all proposed federal wire or oral monitoring applications must receive high-level Departmental and agency review prior to being submitted to a federal district or appeals court. By agreement with Congress and policy, all electronic intercepts of communicative content (except digital display pagers) must receive Departmental review.

A. Federal Investigations

1. **Departmental and Agency Authorization Required:** Pursuant to 18 USC 2516(1), only the high-ranking DOJ attorneys may authorize a federal court application to conduct non-consensual, domestic surveillance of wire or oral communications for law enforcement purposes. The Department of Justice Office of Enforcement Operations' Electronic Surveillance Unit (OEOESU) handles all such requests and, by policy, all requests for electronic intercept of communicative content. A copy of the proposed wire, oral, or electronic intercept order, application, and affidavit is submitted to the OEOESU and to the headquarters office of the investigative agency handling the case. For the USMS, only the Chief, TOG or his superiors may approve Title III requests. Except in the case of genuine emergencies, most original applications require approximately one week to review and process from the time the OEOESU receives the affidavit.
 - a. **Spinoff Requests:** Spinoff requests are applications to conduct electronic surveillance at a new location or over a new facility that are related to an ongoing or previously conducted interception reviewed by the OEOESU, and are considered original applications that require agency and OEOESU approval.
 - b. **Extension Requests:** Extension requests are applications to continue interceptions over the same facility or premises and require review only by OEOESU and not the investigative agency. The OEOESU does not handle state wiretaps or requests to conduct domestic national security electronic surveillance pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 USC 1801, et seq.)(FISA).
2. **Paging Devices Do Not Require Departmental Approval:** By subsequent approval of Congress, Departmental approval to intercept electronic communications to or from digital display pagers is no longer necessary. Application may be made by any federal prosecutor. Agency approval, however, must nonetheless be obtained from a TOG Chief Inspector or his superiors. There are a variety of pager technologies and many communicate their messages through proprietary digital languages or are accompanied by special features (e.g. tone-only pagers are afforded no legal privacy interest and voice-pager messages are considered stored electronic or wire communications). Investigators must know what type of pager they want to intercept in order to determine the necessary legal process.

- B. **State Investigations:** Pursuant to 18 USC 2516(2) and consistent with state law, only the chief state prosecuting attorney (state attorneys general) or principal prosecuting attorneys of state political subdivisions (district attorneys) may make application to a state court to conduct non-consensual, domestic surveillance of wire, oral or electronic communications. There is no state exception to digital-display pagers that would allow assistant district attorneys to make application.

C. Predicate Offenses

Technical Operations Group Topics

1. **Oral and Wire Intercept in Federal Investigations:** The offenses that may be the predicates for a wire or an oral interception order are limited to those set forth in 18 USC 2516(1), which include most serious felonies and, with respect to USMS-primary investigations, include:
 - a. Escape (18 USC 751)
 - b. Obstruction (18 USC 1510)
 - c. Failure to Appear (18 USC 3146)
 - d. Witness Relocation & Protection (18 USC 3521(b)(3)), and
 - e. Fugitive from Justice or Conspiracy investigations for offense identified in 18 USC 2516(1).
 2. **Electronic Intercept in Federal Investigations:** Any federal felony violation may form the basis for an electronic communications intercept. 18 USC 2516(3).
 3. **State Oral, Wire, or Electronic Intercept:** To the extent consistent with state law, most state felony violations (and conspiracy to commit them) may form the basis for communications content intercept. 18 USC 2516(2). Although Escape and Fugitive from Justice are not specifically enumerated in this section, if the applicant can articulate a danger to life, limb or property, the application may meet the requirements of this section.
- D. **Application:** The application, once approved by OEOESU (for federal investigations), must be presented to a federal district court or court of appeals judge and be accompanied by the Department's authorization memorandum. If the investigation involves a state felony offense, the application must be submitted to state court judge as consistent with state law. All applications must comply with the detailed and complex requirements of 18 USC 2518(1).
1. **Identifying Persons To Be Monitored:** Although 18 USC 2518(1)(b)(iv) requires only that the application identify the person(s), if known, committing the offenses and whose communications are to be intercepted, it is Departmental policy to name all persons as to whom there is probable cause to believe are committing the offenses and to delineate who among them will be intercepted over the target facilities discussing the offenses. It is also Department policy to name individuals in Title III pleadings even if their involvement does not rise to the level of probable cause.
 2. **Monitoring Is Necessary:** The application must contain a statement affirming that normal investigative procedures have been tried and failed, or are reasonably unlikely to succeed, or are too dangerous to employ. 18 USC 2518(1)(c). It is not necessary that there be no other normal investigative avenues—only that they have been tried and proven inadequate or have been considered and rejected for the reasons described.
 3. **Surreptitious Entry:** If involving an oral or, occasionally, a wire or an electronic interception, the application must contain a request that the court issue an order authorizing investigative agents to make surreptitious and/or forcible entry to install, maintain, and remove electronic interception devices in or from the targeted premises or vehicle. In effecting this, the applicant should notify the court immediately after each surreptitious entry.
 4. **Changed Numbers:** If involving a wire interception (and an electronic interception involving, for example, a facsimile machine), the application must contain a request that the authorization apply not only to the target telephone number, but to any changed telephone number subsequently assigned to the same cable, pair, and binding posts used by the target landline telephone within the thirty (30) day interception period. With regard to wireless telephones, the language should read: "... but to any changed telephone number or any other telephone number assigned to or used by the instrument bearing the same electronic serial number (ESN) or international mobile equipment identifier (IMEI) used by the target wireless telephone within the thirty (30) day period." The application should also request that the authorization apply to background conversations intercepted in the vicinity of the target telephone while the telephone is off the hook or otherwise in use.
 5. **Mobile Communications:** When the request is to intercept a wireless telephone or a portable paging device, or to install a microphone in an automobile, the affidavit should contain a statement that, pursuant to 18 USC 2518(3), the interceptions may occur not only within the territorial jurisdiction of the court in which the application is made, but also outside that jurisdiction (but within the United

Technical Operations Group Topics

States). Because these devices are easily transported across district lines, this language should be used if there is any indication that the target telephone, paging device, or vehicle will be taken outside the jurisdiction of the court issuing the electronic surveillance order. The order should specifically authorize such extra-jurisdictional interceptions, and should be sought in the jurisdiction having the strongest investigative nexus.

6. **Instructions to Service Provider:** If involving a wire and sometimes an electronic interception, the application must contain a request that the court issue an order directing the service provider, as defined in 18 USC 2510(15), to furnish the investigative agency with all information, facilities, and technical assistance necessary to facilitate the ordered interception. 18 USC 2511(2)(a)(ii) and 2518(4). The application should also request that the court order the service provider and its agents and employees not to disclose the contents of the court order or the existence of the investigation. 18 USC 2511(2)(a)(ii).
7. **Duration:** The application should contain a request that the court's order be issued for a period not to exceed thirty (30) days, measured from the earlier of the day on which the interception begins or ten (10) days after the order is entered, and that the interception must terminate upon the attainment of the authorized objectives. 18 USC 2518(1)(d), (5).
8. **Minimization:** The application should contain a statement affirming that all interceptions will be minimized in accordance with 18 USC 119, as described further in the affidavit.

E. Affidavit: The application must identify the subjects, describe the facility or location that is the subject of the proposed electronic surveillance, and list the alleged offenses that constitute a legal basis for the intercept. It must also establish probable cause that the named subjects are using the targeted telephone(s) or location(s) to facilitate the commission of those offenses or, if a fugitive from justice, to elude capture. In addition to addressing the specific items listed below, the affidavit should mirror the application and address each of the specific requirements listed in 18 USC 2518(1).

1. **Who May Be An Affiant:** The affidavit must be sworn and attested to by an investigative or law enforcement officer, as defined in 18 USC 2510(7). Departmental policy precludes the use of multiple affiants except in rare circumstances. If a state or local law enforcement officer is the affiant for a federal electronic surveillance affidavit, he must be deputized as a federal officer of the agency with responsibility for the offenses under investigation.
2. **Non-Agent Monitors:** The affidavit should identify non-agent monitors because 18 USC 2518(5) permits non-officer "Government personnel" or individuals acting under contract with the government to monitor conversations, but only pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception when monitoring communications, and the affidavit should note the fact that these individuals will be used as monitors pursuant to section 2518(5).
 - a. **Federal Military:** Department of Defense personnel appear to qualify as "Government personnel" and could, therefore, without deputization, assist in the Title III monitoring process (e.g., as translators), if such assistance does not violate the Posse Comitatus laws ("PCA"), 10 USC 375 and 18 USC 1385, and related regulations, 32 CFR 213.10(a)(3), (7). An opinion issued by the Office of Legal Counsel ("OLC"), Department of Justice, dated April 5, 1994, concluded that such assistance by military personnel would not violate the PCA.
 - b. **National Guard:** The foregoing OLC analysis did not extend to National Guard personnel, who are generally considered state employees rather than Federal Government personnel. Consequently, unless National Guardsmen are in a Title 10 active duty status, members of the National Guard will require that they be deputized as law enforcement officers or placed under contract.
3. **Pen/Trap/Toll Data Alone Insufficient:** It is Department policy that pen register or telephone toll information for the target telephone, or physical surveillance of the target premises, standing alone, is generally insufficient to establish probable cause. Probable cause to establish criminal use of the facilities or premises requires independent evidence of use in addition to pen register or surveillance information (e.g. informant or undercover information).
4. **High-Volume Calls To Co-Conspirators:** On rare occasions, criminal use of the target facilities or premises may be established by an extremely high volume of calls to known or suspected

Technical Operations Group Topics

coconspirators or use of the premises by them that coincides with incidents of illegal activity. It is Department policy that the affidavit reflects use of the target telephone or premises within twenty-one days of the date on which the Department authorizes the filing of the application. The subjects' use of the target facilities or premises within the twenty-one-day period may be evidenced through pen register information and/or physical surveillance that update earlier use. Historical information (i.e., information older than six months from the date of the application), combined with pen register information or physical surveillance alone, is generally insufficient to establish probable cause. Pen register information and physical surveillance not only serve to update the probable cause as to the criminal use of a telephone or premises, but also are required (in the absence of other information) to establish the need for the proposed electronic surveillance by demonstrating what types of criminal communications are expected to be intercepted over the telephone or within the premises during the thirty-day authorization period.

5. **Less Intrusive Means and Prior Intercepts:** The affidavit explain why other investigative methods are inadequate and must contain a full and complete statement of any prior electronic surveillance involving the persons, facilities, or locations specified in the application. 18 USC 2518(1)(e). This statement should include the date, jurisdiction, and disposition of previous applications, as well as their relevance, if any, to the instant investigation. In addition to any known prior applications, the TOG inspector conducting the investigation should run a check of USMS electronic surveillance indices, the indices of any other participating agencies, and the indices of any agency which would likely have investigated the subjects in the past. In narcotics investigations, it is the Department's policy that the Drug Enforcement Administration, the Federal Bureau of Investigation, and the United States Customs Service conduct a check to determine if any prior related electronic surveillance has been conducted.
 6. **Duration:** The affidavit must contain a statement of the period of time for which the interception is to be maintained. 18 USC 2518(1)(d). Section 2518(5) provides that an order may be granted for no longer than is necessary to achieve the objectives of the investigation, or in any event no longer than thirty (30) days, whichever occurs first. The statute further provides that the thirty-day period begins on either the day on which investigative officers first begin to conduct the interception or ten days after the order is entered, whichever is earlier. This ten-day grace period is intended primarily for the installation of oral monitoring equipment (microphones), allowing investigators time to break and enter, if necessary, and set up the equipment before the thirty-day period begins to be calculated.
 7. **Minimization:** The affidavit must contain a statement affirming that monitoring agents will minimize all interceptions in accordance with 18 USC 119, as well as other language addressing any specific, anticipated minimization problems, such as the interception of privileged attorney-client communications, or conversations in a foreign language or code. 18 USC 2518(5).
 8. **Privileged Communications:** If any of the named subjects are facing pending state or federal criminal charges, these persons and the nature of their pending charges should be identified in the affidavit, and both the minimization language in the affidavit and the instructions given to the monitoring agents should contain cautionary language regarding the interception of privileged attorney-client conversations.
 9. **Naming Confidential Informants:** Pursuant to the AG's May 30, 2002 Guidelines Regarding the Use of Confidential Informants, investigators shall not name a CI as a named interceptee or a violator in an affidavit in support of an application made pursuant to 18 USC 2516 (Title III) for an electronic surveillance order unless the investigator believes that: (a) omitting the name of the CI from the affidavit would endanger that person's life or otherwise jeopardize an ongoing investigation; or (b) the CI is a bona fide subject of the investigation based on his or her suspected involvement in unauthorized criminal activity. In the event that a CI is named in an electronic surveillance affidavit, the investigator must inform the Federal prosecutor making the application and the Court to which the application is made of the actual status of the CI.
- F. **The Order:** The authorizing language of the order should mirror the requesting language of the application and affidavit, and comply with 18 USC 2518(3), (4), and (5). The court may mandate that the government make periodic progress reports, pursuant to 18 USC 2518(6).
1. **Special Cases:** In the case of a roving interception, the court must make a specific finding that the requirements of 18 USC 2518(11) have been demonstrated adequately. Any other special circumstances, such as extra-jurisdictional interception in the case of mobile interception devices (pursuant to 18 USC 2518(3)) or surreptitious entry should also be authorized specifically in the order.

Technical Operations Group Topics

An order to seal all of the pleadings should also be sought. 18 USC 2518(8)(b).

2. **Technical Assistance Order:** The government should also prepare for the court a technical assistance order to be served on the communication service provider. 18 USC 2511(2)(a)(ii) and 2518(4). This is a redacted order that requires the service provider to assist the agents in effecting the electronic surveillance.

G. Recording and Sealing Required: The contents of any wire, oral, or electronic communication intercepted pursuant to a Title III court order shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any such wire, oral, or electronic communication shall be done in such a way as will protect the recording from editing or other alteration. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing the order and sealed. 18 USC 2518(8)

1. **Sealing:** By Departmental practice, the tapes should be sealed at the end of each interception period, especially if the investigation is lengthy and definitely whenever there is any time gap between extensions. While the statute requires the tapes to be sealed at the "expiration of the period of the order, or extensions thereof," the appellate courts have differed on the amount of time that may elapse between orders before the new order is no longer considered an extension, and, thus, necessitating sealing under the statute. If there is a sealing delay, a good reason for the delay must be provided and the defendant must not have been prejudiced by the failure to timely seal.
2. **Destroying Recorded Intercepts:** The recordings of a communication intercepted pursuant to a Title III court order shall not be destroyed except upon an order of the issuing or denying judge and, in any event shall, be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of 18 USC 2517(1) and (2). The presence of the court's seal provided by 18 USC 2518(8)(b), or a satisfactory explanation for the absence thereof, is a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom. 18 USC 2518(8).

H. Monitors and Minimization

1. **Privileged Communications:** If a monitor intercepts a privileged attorney-client conversation, the monitor should make a notation of that conversation on the log and notify the supervising attorney, who should advise the judge. The tape of the conversation should be sealed and no disclosure of that conversation should be made to other investigative officers.
2. **Foreign Languages:** If any of the named subjects speak a foreign language or converse in code, the statute permits after-the-fact minimization of wire and oral communications when an expert in that code or foreign language is not reasonably available to minimize the conversations contemporaneously with their interception. In either event, the minimization must be accomplished as soon as practicable after the interception. 18 USC 2518(5). Such after-the-fact minimization can be accomplished by an interpreter who listens to all of the communications after they have been recorded and then gives only the pertinent communications to the agent.
3. **Electronic Communications:** After-the-fact minimization is a necessity for the interception of electronic communications over a digital-display pager or an electronic facsimile machine or the internet. In such cases, all communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation. Disclosure is then limited to those communications by the subjects or their confederates that are criminal in nature.
4. **Other Offenses:** When communications are intercepted that relate to any offense not enumerated in the authorization order, the monitoring agent should report it immediately to the AUSA, who should notify the court at the earliest opportunity. Approval by the issuing judge should be sought for the continued interception of such conversations. An order under 18 USC 2517(5) may have to be obtained for testimonial use of "other offense" information.

I. Roving Intercept: Specifically excepted from the particularity requirement of 18 USC 2518(1)(b)(ii) are the roving interception provisions set forth in 18 USC 2518(11). See also 18 USC 2518(12). For roving interception applications, the accompanying DOJ authorization document must be signed by an official at the Assistant Attorney General or acting Assistant Attorney General level or higher. 18 USC 2518(11)(a)(i), (b)(i).

1. **Roving Oral Intercept:** In the case of a roving oral interception, the application must show, and the

Technical Operations Group Topics

order must state, that it is impractical to specify the locations where the oral communications of a particular named subject or subjects are to be intercepted. 18 USC 2518(11)(a)(ii), (iii). Further, monitoring agents must ascertain a specific location before the interception of oral communications begins. 18 USC 2518(12). OEOESU policy allows "spot monitoring" if physical surveillance is not possible.

2. **Roving Wire/Electronic Intercept:** In the case of a roving wire or electronic interception, the application must show, and the order must find, that there is probable cause to believe that the actions of the particular named subject (or subjects) could have the effect of thwarting interception from a specified facility. 18 USC 2518(11)(b)(ii), (iii). Further, the order must limit interceptions to such time as it is reasonable to presume that the target person is or was reasonably proximate to the instrument through which such communication will be or was transmitted. 18 USC 2518(11)(b)(iv). OEOESU policy allows "spot monitoring" if physical surveillance is not possible.

- a. **Phones and Vehicles Crossing District Lines:** 18 USC 2518(3) permits extra-jurisdictional orders in cases involving wireless telephones or vehicles. Thus, all roving orders for phones and vehicles should specify that the order is effective in other jurisdictions.
- b. **When Crossing District Lines Requires A New Order:** While the statute does not address the jurisdictional restrictions of a roving interception, the legislative history suggests—and Department policy concurs—that roving interception authorization is not transjurisdictional with respect to other types of roving intercepts; that is, orders must be obtained in each jurisdiction in which roving interceptions are to be conducted.

- J. **Emergency Title III Intercept:** 18 USC 2518(7), permits the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (Assoc. AG) to specially designate any investigative or law enforcement officer to determine whether an emergency situation exists that requires the interception of wire, oral, or electronic communications pursuant to Title III before a court order can, with due diligence, be obtained.

1. **"Emergency" Defined:** The statute defines an emergency situation as one involving an immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. 18 USC 2518(7). In all but the most unusual circumstances, the only situations likely to constitute an emergency are those involving an imminent threat to life or imminent terrorist activity.
2. **Mechanics of Authorization:** The Criminal Division's emergency procedures require that before the requesting agency contacts the AG, the DAG, or the Assoc. AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division.
 - a. **Through OEOESU:** This approval is facilitated by OEOESU, which is the initial contact for the requesting USAO and the agency. In practice, the emergency procedures are initiated when the AUSA in charge of the case contacts a OEOESU attorney.
 - b. **Agency Concurrence:** After discussions with both the AUSA and the agency headquarters representative responsible for authorization, the OEOESU attorney, in consultation with the OEO Director or an Associate Director, determines whether the statutory requirements have been met. Both OEOESU and the agency's headquarters must agree that an emergency situation and the means to implement the requested electronic surveillance exist. The OEOESU attorney then briefs the AAG or a DAAG and obtains oral authorization on behalf of the Criminal Division. The OEOESU attorney notifies the agency representative and the AUSA that the Division has approved the seeking of an emergency authorization.
 - c. **Contacting the AG, DAG OR ASSOC. AG:** The appropriate agency representative (the Director, Deputy Director or Assistant Director for Investigations) then contacts the AG, the DAG, or the Assoc. AG and seeks permission to make a determination that an emergency situation exists as defined in the statute.
3. **Follow-Up Court Order Within 48 Hours:** The government has forty-eight hours (including weekends and holidays) from the time the authorization was obtained to apply for a court order approving the interception. The package submitted to the court will consist of the AUSA's application, the affidavit, and a proposed order. (This package must be reviewed by the OEOESU before it is submitted to the court.) The affidavit in support of the government's after-the-fact application to the

Technical Operations Group Topics

court for an order approving the emergency interception must contain only those facts known to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved, and be accompanied by a written verification from the requesting agency noting the date and time of the emergency authorization. The government may request, at the time it files for court-authorization for the emergency, court-authorization to continue the interception beyond the initial forty-eight hour period. If continued authorization is sought at the same time, one affidavit may be submitted in support of the emergency application and the extension application, but the affidavit must clearly indicate which information was communicated to the AG, the DAG, or the Assoc. AG at the time the emergency interception was approved and which information was developed thereafter. Two separate applications and proposed orders (one set for the emergency and one set for the extension) should be submitted to the court. If the government seeks continued authorization, that application must be reviewed by OEOESU and approved by the Criminal Division like any other Title III request.

K. Extension Applications: An extension affidavit follows the same format and carries the same statutory requirements as the affidavit that supported the original application. 18 USC 2518(5). The primary difference is in the probable cause section, which must focus on the results obtained (or lack thereof) during the most recent interception period, including any new information regarding the subjects' recent use of the targeted facilities or premises. 18 USC 2518(1)(f).

1. **Discuss New Information:** The affidavit should incorporate by reference the original and all previous extension applications, and then discuss in a paragraph or two the progress of the investigation to date and summarize new information obtained during the past thirty days. If no relevant interceptions were made during the previous period, a sufficient explanation must be provided to the court (for example, technical or installation problems with monitoring equipment, or the physical absence of the subject during all or part of the interception period), along with a reasonable, factually based explanation of why the problems are expected to be rectified during the next thirty days. A sampling of recent interceptions sufficient to establish probable cause that the subjects are continuing to use the targeted facilities or location in furtherance of the stated offenses should then be described. The affidavit should not contain verbatim transcripts or a series of pieced-together progress reports; rather, selected and paraphrased or highlighted portions of a few key, criminal conversations should be set forth, along with an explanation, if necessary, of the context in which the conversations were spoken, and the affiant's opinion (based on training and experience) of their meaning if they are in code or are otherwise unclear. The excerpted conversations should reflect results obtained over the bulk of the thirty-day period, and not consist solely of interceptions obtained, for example, during the first ten days. The most recent excerpt of an intercepted communication should be, if possible, within seven calendar days of when the Title III application is submitted to the Criminal Division for approval. If there are no recent interceptions, the affidavit should include a brief explanation as to why that is the case.
2. **Why Intercept Is Still Necessary:** The "Need for Interception and Alternative Investigative Techniques" section should state that the facts set forth in the original affidavit regarding the exhaustion of alternative investigative techniques are continuing and should cite examples of what additional efforts have been made during the preceding interception period and explain why the electronic surveillance conducted thus far has been insufficient to meet the goals of the investigation. It may also be necessary to add or delete subjects and offenses due to new information learned from the interceptions. An indices check must be done for any additional names.
3. **Break In Monitoring:** When caused by administrative difficulties, a brief hiatus between the expiration of an order and the extension will not prevent the extension from being deemed an "extension" within the meaning of section 2518(8)(a).
4. **Allow Time for OEOESU Review:** Title III does not limit the number of extension affidavits that may be filed. OEOESU can usually review and process extension applications in three to four days. If it is important that the electronic surveillance not be interrupted between orders, the extension request should be submitted to OEOESU with sufficient lead time.

L. Spinoff Applications: New applications arising from the same investigation to conduct electronic surveillance over additional facilities are considered original requests, even though the same subjects are targeted, and are reviewed and processed by both OEOESU and the investigative agency.

1. **New Facility:** A new facility is one which, in the case of landline telephones, is carried over a different cable, pair, and binding posts, or, in the case of cellular telephones, over an instrument bearing a different electronic serial number/international mobile equipment identifier (and/or telephone

Technical Operations Group Topics

number) than that of the originally authorized facility.

2. **New Landline Number:** If a targeted landline telephone is given a new telephone number during an interception period but maintains the same location (the same cable, pair, and binding posts), it is not considered a spinoff and applications for additional thirty-day interception periods are extensions of the original authorization (the court should be notified of the number change).
3. **Discuss New Information:** As with extension requests, prior affidavits in the same investigation may be incorporated by reference. The probable cause section in the spinoff application should focus on the newly targeted facility or location and any additional subjects. If new subjects are added, an indices check must be done for their names.
4. **Why Intercept Is Still Necessary:** A spinoff application may not merely incorporate by reference the "Need for Interception and Exhaustion of Alternative Techniques" section of the original affidavit. This section must address the facts as they apply to the spinoff application.
5. **Minimization Language:** The minimization language of the original affidavit should be reviewed to ensure that it comports with any new facts particular to the new facility or location.

M. Progress Reports: 18 USC 2518(6) provides for periodic progress reports to be made at the judge's discretion. These are generally at five-, seven-, or ten-day intervals, and should contain enough (summarized) excerpts from intercepted conversations to establish continuing probable cause and need for the surveillance. Any new investigative information pertinent to the electronic surveillance, such as newly identified subjects or the addition of new violations, should be brought to the court's attention in the progress reports and be included in the next extension request.

N. Inventory Notice: 18 USC 2518(8)(d) requires an inventory notice to be served on persons named in the order, and "...other such parties to intercepted communications as the judge may determine ... is in the interest of justice ..." within a reasonable time, but not later than 90 days after the end of the last extension order. The government has an obligation to categorize those persons whose communications were intercepted so that the judge may make a reasoned determination about whether they will receive inventory notice. Upon a showing of good cause (e.g., impairment of an ongoing investigation), the court may delay service of inventory notice.

O. Disclosing Title III Evidence

1. **Law Enforcement Use:** 18 USC 2517(1) authorizes an investigative or law enforcement officer to disclose, without prior court approval, the contents of intercepted communications to another law enforcement or investigative officer (as defined by 18 USC 2510(7)). 18 USC 2517(2) permits an investigative or law enforcement officer, without prior court approval, to use the contents of properly obtained electronic surveillance evidence to the extent that such use is appropriate to the proper performance of his official duties.
2. **For "Good Cause":** When in doubt about whether the disclosure or use of electronic surveillance evidence is permitted, obtain a court order pursuant to 18 USC 2518(8)(b) authorizing the disclosure and use for "good cause." The Department recommends this course of action because 18 USC 2520 provides that a good faith reliance on a court order is a complete defense to civil and criminal actions for unauthorized disclosure of electronic surveillance information. This order will allow an investigator to disclose electronic surveillance information to certain foreign law enforcement officials (to the extent consistent with U.S. diplomatic policy).
3. **Testimonial Use:** 18 USC 2517(3) allows a person, without prior court approval, to disclose electronic surveillance information, or any derivative evidence, while giving testimony under oath in any federal, state, or local proceeding.
4. **Privileged Communications:** 18 USC 2517(4) provides: "No other privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."
5. **"Other Crimes" Evidence:** 18 USC 2517(5) pertains to the interception of conversations that relate to offenses other than those specified in the authorization order. In pertinent part, that section states: "When ... a law enforcement officer ... intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order ..., the contents thereof, and evidence derived

Technical Operations Group Topics

therefrom, may be disclosed or used [for law enforcement purposes] ..." or disclosed under oath in any proceeding when the "... judge finds on subsequent application that the contents were otherwise intercepted in accordance with [Title III]." The purpose of section 2517(5) is to ensure that the interception of the other offenses was truly incidental to the interception of offenses for which the government had court-authorization.

VIDEO SURVEILLANCE AND OPTICAL DEVICES

Video surveillance, the use of closed circuit television (CCTV), or any other device to enhance the optical observation of a person is not regulated by Title III, but may be a part of an application for electronic surveillance. A court order and prior Department approval are required unless (i) there is a consenting party present at all times, or (ii) there is no Fourth Amendment reasonable expectation of privacy (e.g. the surveillance is used to record events in public places or places where the public has unrestricted access and where the camera equipment can be installed in places to which investigators have lawful access).

- A. **Consensual CCTV Installation and Monitoring:** Consensual video surveillance does not violate the Fourth Amendment and, therefore, no court order is required. CCTV equipment may be installed without a court order in a non-public area with properly obtained consent. As with all consenting surveillance, any viewing of video surveillance must be stopped when the consenting party is absent from the viewing area. Consent should be written and forwarded to a TOG inspector with the monitoring request. Once the request is approved, TOG will conduct the installation. If special concealment techniques are required, the investigator should contact a TOG inspector as soon as possible. Whenever possible, investigators should provide still photographs, videotape, or even drawings of the surrounding area to be monitored.
- B. **Non-Consensual Video Surveillance:** CCTV surveillance of constitutionally protected areas requires a court order authorizing the installation and monitoring of the area. If a court order is required, the pleadings are to be based on Rule 41(b) of the Federal Rules of Criminal Procedure and the All Writs Act (28 USC 1651). Investigators should contact a TOG inspector as soon as possible for assistance in preparing the court order, application and affidavit. Many circuits require that applications to use video surveillance of suspected criminal activities meet most of the higher constitutional standards required under Title III. Therefore, the application and order should usually be based on an affidavit that establishes probable cause to believe that evidence of a federal crime will be obtained by the surveillance, and should also include: (1) a statement indicating that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or are too dangerous; (2) a particularized description of the premises to be surveilled; (3) the names of the persons to be surveilled, if known; (4) a statement of the steps to be taken to ensure that the surveillance will be minimized to effectuate only the purposes for which the order is issued; and (5) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization, or in any event no longer than thirty days (a ten-day grace period is not permitted; the time period begins to run from the date of the order).
- C. **Non-Consensual Video with Oral Intercept:** The same affidavit may be used to establish probable cause for the use of both the microphone and the camera. Separate applications and orders, however, should be filed for each type of interception because each is governed by a different standard. See Title III Communications Intercept for detail.

WIRELESS/CELLULAR ANALYZERS & RECEIVERS

b2/7E [REDACTED] can [REDACTED]
When a wireless telephone is used to send or receive a call, collectible data includes [REDACTED]
[REDACTED]

- A. **PEN/TRAP Order Required:** 18 USC 3127 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information. Therefore, a pen register/trap and trace order must be obtained to use a government [REDACTED] to capture wireless call data. To the extent that such devices may be configured to intercept communications content, such use must be pursuant to a Title III court order.

- B. **Requesting Tog Assistance:** Because [REDACTED] are complex and [REDACTED]

Technical Operations Group Topics

b2/7E

[REDACTED] investigators should contact a TOG inspector as soon as possible to discuss specific applications and [REDACTED]

GOVERNMENT-INSTALLED TRACKING DEVICES

- A. Obtain a Court Order:** Tracking devices are not regulated by Title III, but their use is governed by existing case law. A search warrant or court order is needed only when the object to which the tracking device is attached enters an area that carries a legitimate expectation of privacy, such as the inside of a vehicle or a private residence—or if clandestine installation, maintenance and retrieval is required. Since it often cannot be determined in advance whether a package containing a tracking device will be taken inside a place where a person has a Fourth Amendment expectation of privacy, a court order should almost always be obtained to assure both the admissibility of evidence as well as the device's legal installation, maintenance and retrieval. Investigators should consult with a TOG inspector as soon as possible to discuss their requirement and prepare the court order and affidavit. A court order issued for such a device is valid anywhere within the United States. 18 USC 3117.
- B. Aircraft Transponders:** A transponder is a special type of beacon transmitter used for tracking aircraft. The use of this type of device requires close coordination with the FAA. Due to the complexity of installing transponders on aircraft, installations will only be performed by FAA-certified personnel. Investigators requiring this type of equipment shall provide a TOG inspector as much notice as possible. Close coordination between EPIC, FAA and TOG will be maintained during the monitoring operation. If court ordered surreptitious entry is required to perform the installation, TOG inspectors will provide the access required to the FAA-certified technician. The same caveats regarding Fourth Amendment rights mentioned in vehicle tracking beacons apply to aircraft transponders.

TECHNICAL SURVEILLANCE COUNTERMEASURES

Authorized TOG personnel and others designated by the Chief, TOG will be the only participants to conduct Technical Surveillance Countermeasure (TSCM) activities. Personnel who conduct TSCM surveys will be limited to those that have been through formal and approved TSCM training. The USMS component involved in processing, discussing, and/or storing Classified National Security Information (CNSI), restricted data, or unclassified but sensitive information shall, in response to a specific threat and based on risk management principles, determine the need for a TSCM survey. To obtain maximum effectiveness within the various TSCM programs, the USMS will exchange technical information, coordinate programs, practice reciprocity, and participate in consolidated programs, when appropriate.

- A. TSCM Survey Procedures:** The practices, procedures, applications, equipment, and principles of a TSCM survey are classified and are outlined in a separate USMS document entitled "USMS Technical Surveillance Countermeasures Procedural Guide."

b2/7E

- B. Locations To Be Surveyed:** The Technical Operations Group (TOG) will conduct TSCM surveys only in [REDACTED] or locations as designated by the Assistant Director for the Investigative Operations (IOD) or the Chief, Technical Operations Group (TOG).

- C. TSCM Methodology:** TSCM surveys will be conducted by TOG using the following methodology:

b2/7E

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

- D. Requests for TSCM Survey:** Requests of the Technical Operations Group (TOG) for a Technical Surveillance Countermeasures (TSCM) survey will be handled in the following manner:

1. **Requests Shall Be Safeguarded:** All TSCM requests will initially be treated as [REDACTED] information. Only key personnel (Director, Deputy Director, Assistant Director, U. S. Marshal, and/or

b2/7E

Technical Operations Group Topics

Chief) should have knowledge of a TSCM survey. Any other individual will only have access on a "need to know" basis. Upon arrival for the TSCM survey, the team conducting the inspection will provide a briefing to all other personnel with a "need to know."

b2/7E

2. **Transmitting the Request:** Requests will be forwarded to the Chief, Technical Operations Group (TOG), [REDACTED]. When using certified mail, insure that all appropriate regulations for sending [REDACTED] information are followed.

b2/7E

E. **TSCM Survey Findings and Reporting Requirements:** All findings will be reported based upon the TSCM survey. Findings fall into one of the following three categories:

b2/7E

1. [REDACTED]. The report will be submitted to the Chief, TOG and to the Division Assistant Director/Chief Deputy for the facility or space surveyed.

b2/7E

2. [REDACTED] All aspects of the [REDACTED] will be noted with [REDACTED]. The report will be submitted to the Chief, TOG and to the Division Assistant Director/Chief Deputy for the facility or space surveyed.

b2/7E

3. [REDACTED] If this category finding is discovered, [REDACTED]

AERIAL SURVEILLANCE

TOG's Air Surveillance Operations (ASO) maintains aircraft to support critical missions for the Investigative Operations Division. It also provides limited support to other divisions and assists other federal, state and local agencies and departments. All deployments are subject to approval by the Chief, TOG.

A. **Purposes of Flight:** TOG aircraft shall only be used for the following functions and purposes that are in support of criminal investigations conducted by the Investigative Operations Division, TOG, or other authorized entities as set forth herein:

1. Aerial Surveillance (tracing suspects, associates, and other violators)
2. Electronic Tracking (DF tracking of transmitters and beacons)
3. Aerial Photography and Transmission of Photo-Images
4. Communications Platform (aerial repeater, monitoring body-wire and other transmitters).
5. Special Missions in support of Investigative Operations Division operations (including Special Operations Group) as authorized by the Chief, TOG or his superiors.
6. Emergency Missions (such as search & rescue and national or local disasters) as authorized by the Chief, TOG or his superiors.
7. Ferry (delivery, transfer, maintenance).
8. Support of other federal, state or local agencies or departments authorized by the Chief, TOG, his superiors or designee.

Technical Operations Group Topics

9. Flight Training, Currency and Evaluation.

10. Other missions as authorized by the Chief, TOG, his superiors or designee.

B. Who May Fly: Individuals will be designated to participate in TOG flights under one of the following criteria:

1. Criminal investigators assigned full-time to TOG or as a collateral duty, specifically requiring participation in flight activities on a full-time or primary-duty basis.
2. Other USMS criminal investigators or employees participating in observer, photo, communications activities (non-pilot positions) on a voluntary basis with district or supervisory approval.
3. Employees of other federal, state and local agencies participating in an observer, photo, communications activities (non-pilot positions) who have obtained approval from their agencies and the Chief, TOG.

C. Detailed Operating Procedures: TOG shall develop and maintain its own internal operating procedures with respect to its flight program, certification, maintenance and aircraft operational use, use of aircraft and passengers, pilot and crew qualifications and training requirements, routine, operational, emergency and distress procedures (which shall be properly marked and safeguarded), and any other matter effecting the safe and economical deployment of its aviation resources.