



HOMELAND SECURITY  
INVESTIGATIONS TECHNICAL OPERATIONS – TITLE  
III & NON TITLE III TRANSLATION /  
TRANSCRIPTION PROGRAMS



ICE



# TITLE III – WHAT IS A TITLE III INVESTIGATION - WIRETAP

Title III: The lawful interception of communications, commonly referred to as “wiretaps.”

- Land-lines
- Fax Machine
- Cellular Phones (including text\*)
- Emails
- Internet Service Providers
- Voice Over IP (VOIP)



# I WANT TO WIRETAP YOU





## TITLE III – WIRETAP VS. 4<sup>TH</sup> AMENDMENT

A wiretap would normally violate the Fourth Amendment prohibition against unreasonable searches.

- Because of the intrusive nature of electronic surveillance, a court order is needed for each request. To obtain a court order, an affiant must demonstrate both **PROBABLE CAUSE** that target subjects are using a target device to commit the stated offenses as well as the **NECESSITY** for a wiretap within 21 days of DOJ approval in order to achieve investigative goals.





## TITLE III – STATUTORY HISTORY



CALEA: Communications Assistance for Law Enforcement Act – Adopted in 1994 Amends both the Title III of The Omnibus Crime Control and Safe Streets Act of 1968 “Wiretap Act” and the Electronic Communications Privacy Act (1986) CALEA also has provisions relating to email and Internet Service Providers (ISPs)



# TITLE III – PREDICATE OFFENSES

Title 8 USC 1324, 1327, and 1328 Title 18 USC 115 Retaliation Against  
Bribery of Public Officials Title 18 USC 659 Theft from Interstate Ship  
of Institution or Officer Title 18 USC 1956 and 1957 Money Laundering  
USC 1963 Racketeer Influenced and Corrupt Organizations Title 18 USC 2251  
Children including Material Title 18 USC 3146 Penalty for Failure to  
Act Title 31 USC 5322 Criminal Penalties [with respect to monetary  
Peonage Title 18 U.S.C. § 1584 Involuntary servitude Title 18 U.S.C. 2251  
Trafficking with respect to peonage, slavery, involuntary servitude,  
conduct with respect to documents in furtherance of trafficking, peonage,  
labor.





## TITLE III - DEFINITIONS

### Interception

A communication is 'intercepted' if a device is used by a third party to acquire any information concerning the substance, purport or meaning (i.e., the "content") of that communication.



### Device

A 'device' is anything that does the job of acquiring the content of any wire, oral, or electronic communication.





## TITLE III - DEFINITIONS

### Oral Communication

Any transmitted spoken communication where the speaker has a reasonable expectation of privacy in that speaking and that does not constitute electronic communication.

### Wire Communication

Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

### Electronic Communication

any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce, but does not include: any wire or oral communication, any communication made through a tone-only paging device, any communication from a tracking device (as defined in section 3117 of this title), or electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.





## TITLE III - DEFINITIONS

### Interceptee

Anyone intercepted off your wiretap. The interceptee does not need to be identified and may in fact be listed as “FNU LNU using the moniker “Shoestring.”

### Dirty Call

An intercepted and recorded or documented communication between two or more individuals / co-conspirators, either electronic or wire, which conveys the intent or completion of a predicate offense listed in your wiretap. This is your proof the communication device your asking to intercept is in fact used to facilitate the predicate offense(s). A dirty call can be a recorded conversation or text messages. (Other wiretap, Undercover agent, Confidential Informant) Must be within the last 6 months by the time the affidavit is signed off on by the DAAG (Deputy Assistant Attorney General) at OEO / Main DOJ.





## TITLE III - DEFINITIONS

### Dirty Toll

A contact within a target devices documented communications which: Occurred within 21 days of the DAAG review (final stage before judge's signature), Shows the target device is communicating with another "dirty" device. Must be able to show the nature of the dirty communication. Department of Justice, Office of Enforcement Operations (DOJ-OEO) requires three to six contacts from your subject \*\*\*





## TITLE III – WHY AM I WORKING THIS HARD?

The Truth: Certain levels of targets are only going to be caught through Title III investigations.



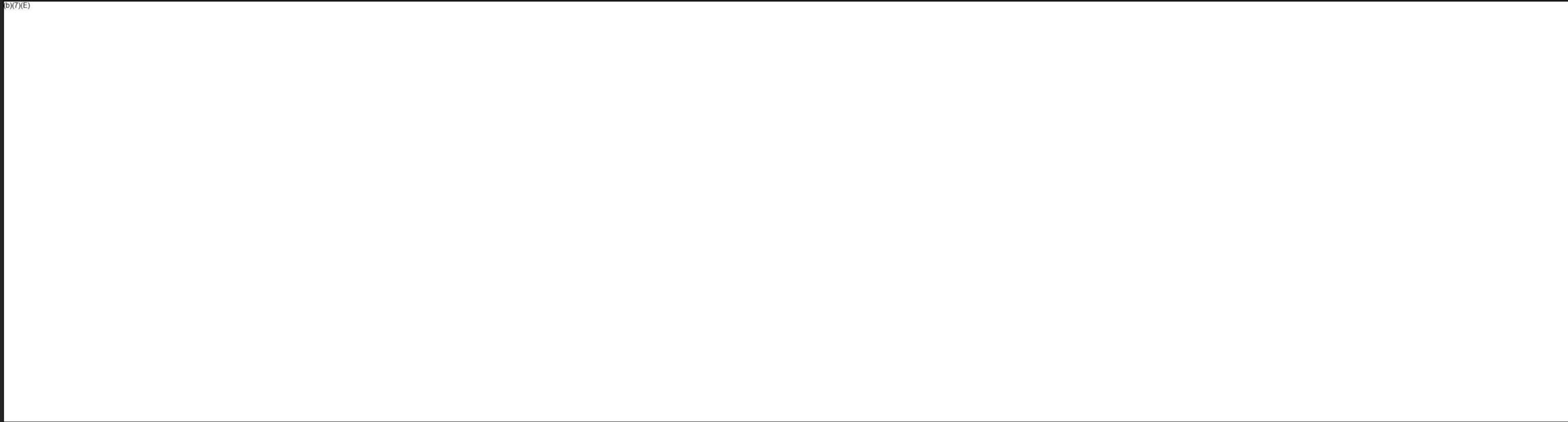


## TITLE III – ADDITIONAL CONSIDERATIONS

Logistics, Resources, Personnel, and Support



(b)(7)(E)





## TITLE III – PROSECUTORIAL PARTNERSHIP

The assigned prosecutor or Assistant United States Attorney (AUSA) is now your **PARTNER.**

Who is Writing the Affidavits: Some districts the case agent writes, others the AUSA / Prosecutor writes  
Timelines: There are certain expectations for timeliness. **EVERYTHING** you do in a wiretap has either a deadline or expiration date. (Pen Registers, 15 Day Reports, usefulness of “dirty calls and tolls”)  
Review Process Federal: AUSA, Supervisor, Chief, DOJ / OEO, OPLA / Tech. Ops , DAAG  
Review Process State: Prosecutor, Supervisor, OPLA / Tech. Ops





## TITLE III – AFFIDAVIT & LEGAL REQUIREMENTS

Each Affidavit must have the following.

Generally speaking each affidavit will follow the same format in regards to the below sections. EACH district, state and federal, will have their own unique format as preferred by either the prosecutors or judges. There is NO way to standardize the format, just the content.

b)(7)(E)



# TITLE III – AFFIDAVIT & LEGAL REQUIREMENTS ... CONTINUED

(b)(7)(E)





## TITLE III – THE PROCESS

- Case Agent prepares Affidavit First Draft sent to AUSA  
Affidavit to first line supervisor Affidavit sent to DOJ/OEO  
(depending on type) OEO approves wire interception ser  
and AUSA swear to the affidavit and application to the Ju  
officers authorize the wire interception





## TITLE III – THE PROCESS – ELECTRONIC SURVEILLANCE (ELSUR) CHECKS

What is an ELSUR indices check?

- Checking names, phone number, emails, IP address, ESN numbers, etc for prior Title III orders. These checks must be completed before the affidavit is presented to the judge. Required under 18 USC 2518(1)e. Each federal agency and each federal Title III complies with these checks. Tech. Ops. maintains the responsibility for authenticating ELSUR checks through the ELSUR program.





# TITLE III – THE TIMELINE



(b)(7)(E)





# TITLE III – REQUIREMENTS OF TECH. OPS.

ONCE THE JUDGE HAS SIGNED AND DATED THE TITLE-III COURT ORDER SEND THE T-III PROGRAM MANAGER A COPY OF ALL SIGNED COURT DOCUMENTS ASAP!! COURT ORDER / APPLICATION / AFFIDAVIT/ DAAG LETTER VIA EMAIL WITHIN 24 HOURS [REDACTED]@DHS.GOV



DONE at Houston, Texas, on this 20 day of November, 2009,

[REDACTED]

UNITED STATES DISTRICT JUDGE  
SOUTHERN DISTRICT OF TEXAS

10

TRUE COPY I CERTIFY

[REDACTED]





# TITLE III – CASE MANAGEMENT

EVENT LOG / <span style="border: 1px solid black; padding: 2px;">(b)(7)(E)</span>		0				
Date	Time	Event Summary	Pole Camera	Session Number	Photos	PHX Case Number
05/02/09	1954	(b)(6), (b)(7)(C), (b)(7)(E)				
05/03/09	740					
05/03/09	758					
05/03/09	1036					
05/04/09	655					
05/04/09	839					
05/04/09	839					



Page 2358

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2359

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2360

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2361

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2362

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2363

Withheld pursuant to exemption

(b)(6) ; (b)(7)(C) ; (b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2364

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act