US Immigration and Customs Enforcement
OFFICE OF TRAINING AND DEVELOPMENT

ICE Academy

ELECTRONIC SURVEILLANCE
11400

Student Guide

HSI Special Agent Training

Electronic Surveillance

Motivation

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 set the rules for obtaining wiretap orders in the United States. It also set forth that any non-consensual interception, disclosure, or use of the content of any wire, oral, or electronic communication is prohibited without court order. This Act applies to law enforcement as well as to private individuals.

Only crimes Only crimes enumerated in Title 18, United States Code (USC), Section 2516(1), can be investigated through wire, oral or electronic communications; the willful act of intercepting or attempting to intercept any wire, oral, or electronic non-consensual communications without a court order can result in a penalty with a maximum of 5 years imprisonment – 18 USC 2511(1).

In this lesson we'll look at the fundamental aspects of electronic surveillance, starting with the differences between consensual and non-consensual monitoring. You'll learn the basic procedure of selecting electronic surveillance equipment. We'll also use the Technical Operations Handbook (HB 14-04) as a collaborating tool to review the policies, procedures, and technical guidance associated with using technology to bolster your investigations.

Objectives

Terminal Performance Objective (TPO)

Conditions: Given a set of case-related facts and access to a Technical Enforcement Officer (TEO)/Designated Technical Agent (DTA),
Behavior: demonstrate the ability to prepare for and conduct an electronic surveillance in support of an investigation
Criterion: following the techniques and procedures in accordance with the HSI Technical Operations Handbook.

Enabling Performance Objectives (EPOs)

EPO #1: Distinguish between all-parties consent, consensual and non-consensual monitoring.
EPO #2: Determine Department of Justice, Department of Homeland Security and HSI policies and procedures for the interception and/or recording of consensually monitored verbal communications.
EPO #3: Identify HSI policies and procedures for the issuance and control of electronic surveillance equipment and evidence.
EPO #4: Use basic functions of selected electronic surveillance equipment, including (b)(7)(E)

Review of the Past

As was pointed out in physical surveillance, planning is essential to any surveillance investigation. You also learned that the objectives of surveillances will always dictate the methods you use. A few examples of those objectives included:

- Obtaining evidence
- Corroborating allegations
- Identifying associates and co-conspirators
- Establishing probable cause

You also talked about the many different types of surveillance. One type discussed in particular was electronic surveillance – gathering subject-related information and/or evidence through the use of technical devices. Additionally (b)(7)(E) (b)(7)(E)

You examined the *Policy Concerning Electronic Recording of Statements in Federal Criminal Investigations* in the Interviewing Lesson, both in CITP and in HSISAT.

Advance Organizer of Main Ideas

This lesson focuses primarily on the various types of electronic surveillance equipment, specifically c(b)(7)(E) (b)(7)(E) You will have the opportunity to become familiar with the basic operation of electronic surveillance equipment and its applications in the investigation of criminal activities; and to implement what you learn in a lab session outside of the classroom.

Agenda

In this lesson, you will:

- Use the Technical Operations Handbook as a guide to cover the concepts of Electronic Surveillance since it contains much of the information you will need to know when you get to the field.
- Pay particular attention to areas that may typically result in procedural or legal errors.
- Discuss the differences between consensual and non-consensual monitoring and what is meant by “all party consent.”
- Discuss the Department of Justice, HSI policies and procedures for the interception and/or recording of consensually monitored verbal communications, as well as HSI policies and procedures for the issuance and control of electronic surveillance equipment and handling electronic evidence.
- Discuss the basic functions of selected electronic surveillance equipment, including (b)(7)(E)
  - The instructor will demonstrate how to use the equipment while students then learn how to use the basic functions.
  - You will then have an opportunity to practice using the equipment. This includes performing equipment check prior to usage.

- In a later lab session you will have an opportunity to practice for field conditions. They will work in groups and receive sets of instructions that require them to monitor and record consensual phone calls and several "meets" with violators in public venues. They will return to the classroom and make a CD of the "evidence" they have gathered and make a copy with (b)(7)(E)

INSTRUCTION

Explanation

If you anticipate the use of electronic surveillance, you should establish contact with the Technical Enforcement Officer (TEO) or Designated Technical Agent (DTA) as early in the planning stage as possible. In addition to their technical expertise, TEOs/DTAs are very familiar with the various legal and administrative considerations involving electronic surveillance. You will require support in those areas.

You use the Technical Operations Handbook as the primary guide for instruction. "The Technical Operations Handbook establishes policies and procedures, as well as technical guidance, to be followed by U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Technical Enforcement Officers (TEOs), Special Agents (SAs), Intelligence Research Specialists (IRSs), and other HSI employees when conducting or supporting investigations involving the use of electronic surveillance equipment and software in compliance with applicable laws, regulations, and policies." It contains most of the important information and instruction that SAs will need in the field.

A. EPO #1: Distinguish between all-parties consent, consensual and non-consensual monitoring**.**

1. Non-Consensual Monitoring

   a. Criminal offense to willfully intercept or attempt to intercept any wire or oral non-consensual communications without a court order (18 USC 2511(1)). Penalty is a maximum of 5 years of imprisonment.
   b. Non-Consensual Monitoring – no parties to the conversation have consented to the monitoring – also referred to as a wiretap or Title III intercept (18 USC 2510–2522).

Notes:

2. Consensual Monitoring *(Chapter 9.1)*
This lesson concentrates on consensual monitoring.

a. Consensual monitoring – at least one party to a communication has consented, and the consenting party is directly or indirectly working for the government, e.g., undercover agent or informant.
b. Consensual monitoring generally does not require a court order but does require administrative authorization.

Note: Exception – Some judicial districts require a court order to consensually monitor telephone conversations, where the interception of conversations are monitored and recorded remotely. Always consult the local AUSA.

Example: (b)(7)(E)
(b)(7)(E)

c. All party consent – all parties to a conversation have consented for the conversation to be recorded, e.g., an interview.
d. The terms "interception" and "monitoring" mean the aural acquisition of oral (verbal) communications by use of an electronic, mechanical, or other device.
e. For a consensually intercepted conversation to be utilized in a court proceeding, the burden is on the U.S. government to prove that one of the parties of the conversation had given voluntary prior consent to the interception.
f. Establishing consent is imperative.

Notes:

3. Consent can be established and documented by at least two methods:

a. (b)(7)(E)
b.

Note: (b)(7)(E)

Notes:

B. EPO #2: Determine Department of Justice and HSI policies and procedures for the interception and/or recording of consensually monitored verbal communications.

1. Consensual Monitoring Authorization Process

a. Approval

1) The Department of Justice delegated the authority to approve consensual interceptions to the head of the investigative agency or their designee.
2) The agency is responsible for supervising, monitoring, tracking, and approving all consensual monitoring of oral communications.
3) HSI Consensual Monitoring Requests/Notifications and Reports of Use are documented and approved using the (b)(7)(E)
4) The Department of Justice requires prior written approval when any participant involved in an electronic surveillance falls within certain "Sensitive Categories" established by the Attorney General.

a) Oral authorization requests may be made to the Director or Associate Director of the DOJ Criminal Division's Office of Enforcement Operations in emergency situations. Headquarters will coordinate.

Notes:

b. Sensitive Categories *(Chapter 9.5)*

1) Whenever any participants involved in an electronic surveillance fall under a sensitive category, written DOJ approval is required.

2) Electronic surveillance is not initiated until a written request is submitted to Headquarters and subsequently approved by the DOJ.
3) The sensitive categories requiring written approval of the Attorney General or designee:

a) A member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years
b) A 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 involves bribery, conflict of interest, or extortion relating to the performance of his/her official duties
c) Any party who is/was a member of federal Witness Security Program (WSP) and that fact is known to the agency involved or its officers
d) Member of foreign country's diplomatic corps
e) Any consenting or non-consenting party in the custody of the U.S. Marshal's Service or the Bureau of Prisons
f) The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the U.S. Attorney in the district where the investigation is being conducted requests the investigative agency to obtain prior written approval for making a consensual interception in a specific investigation

Notes:

c. Authorization Procedures and Rules – all consensual monitoring requests require the following documentation:

1)
2)
3)

(b)(7)(E)

(b)(7)(E)

Notes:

Note: (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

Notes:

e. Non-telephone intercepts

1) Face-to-face conversations considered to have a higher expectation of privacy than a telephone conversation
2) Have higher approval level
3) Authorization – Head of Agency or designee in advance unless:

a) All parties to the conversation consent, or
b) Exigent circumstances preclude advance authorization, e.g., imminent loss of essential evidence or threat to the immediate safety of SA or confidential source.
c) Time frame: Special Agents shall have an approved (b)(7)(E) prior to conducting a non-telephonic intercept.
d) When exigent circumstances prevent prior entry and approval in (b)(7)(concurrent verbal approvals required.

(1) Special Agent's First Line Supervisor
(2) Assistant United States Attorney

Note: (b)(7)(E)
(b)(7)(E)

e) In a continuing investigation, requests may be made and approved for a 30-day period.
f) (b)(7)(E)
g) In accordance with the Technical Operations Handbook, a "Report of Use" *(Chapter 9.4)* must be submitted (b)(7)(E) immediately upon termination of the authorized interception period.

Notes:

2. Telephone intercepts

   a. Approval: Head of the Office
   b. Special Agents shall have an approved (b)(7)(E) prior to conducting a telephonic intercept.
   c. When exigent circumstances prevent prior approval (b)(7)(E) concurrent verbal approvals required

      1) Special Agent's own authority with notification to the first-line supervisor at the first available opportunity
      2) Assistant United States Attorney

Note: (b)(7)(E)
(b)(7)(E)

Note: (b)(7)(E)
(b)(7)(E)

   d. Assistant U.S. Attorney advice is required for each ELSUR interception period.
   e. In accordance with the Technical Operations Handbook, a "Report of Use" must be submitted (b)(7)(E) immediately upon termination of the authorized interception period.

Notes:

C. EPO #3: Identify HSI policies and procedures for the issuance and control of electronic surveillance equipment and evidence.

1. Electronic surveillance equipment – electronic devices that may be used to collect evidence *(Chapter 4.7)*

   a. Includes, but not limited to:

(b)(7)(E)

Notes:

   b. Does not include:

(b)(7)(E)

Notes:

2. The Designated Technical Agent (DTA) is the SA who supports criminal investigations through electronic surveillance and techniques, Technical Operations Handbook 14-04 *(Chapter 4.2)*.
3. Technical Enforcement Officer (TEO)

    a. Primary LEO who supports criminal investigations through the use of electronic surveillance equipment and techniques
    b. Primary responsibility is the gathering of evidence in furtherance of criminal prosecutions, Technical Operations Handbook 14-04 *(Chapter 4.22)*

Notes:

4. Storage and Issuance – (b)(7)(E)

    a. (b)(7)(E)

    b.

Notes:

5. Use of Other Agencies *(Chapter 19.1)*

    a. Unless authorized by Tech Ops, only HSI equipment and installers will be used.
    b. Obtaining equipment and assistance from other agencies:

        1) (b)(7)(E)
        2)
        3)

Notes:

D. EPO #4: Use basic functions of selected electronic surveillance equipment, including (b)(7)(E)

(b)(7)(E)

Page 2180

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2181

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2182

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2183

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2184

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2185

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

(b)(7)(E)

Notes:

Demonstration

The instructor will demonstrate how to find information in the Technical Operations Handbook, including policies and procedures for typical electronic surveillance circumstances Only crimes Only crimes enumerated in Title 18, United States Code (USC), Section 2516(1), can be investigated through wire, oral or electronic communications; the willful act of intercepting or attempting to intercept any wire, oral, or electronic non-consensual communications without a court order can result in a penalty with a maximum of 5 years imprisonment – 18 USC 2511(1).

You should have the following technical surveillance equipment for the demonstration:

(b)(7)(E)

You will use all this equipment in the Electronic Surveillance Lab. During the demonstration, you should demonstrate all the equipment and review its usage. You will demonstrate specific equipment; and then you will have an opportunity to practice on their own.

The instructor will also demonstrate the basic operation of the following devices. You should have access to the equipment so they can follow along.

(b)(7)(E)

Student Practice

The student practice in this lesson applies to the recording and transmitting technology. You have the opportunity to handle and use the various devices within the classroom setting. They (b)(7)(E) This practice time enables you to take full advantage of practical application lab that follows which allows them to use the equipment in simulated field conditions.

You should have the following technical surveillance equipment available to practice.

(b)(7)(E)

The instructor will have you form three groups. Each group will be assigned one of each of the above pieces of equipment. You should take the opportunity to handle and use the various devices. You should:

(b)(7)(E)

The student practice in this lesson applies to the recording and transmitting technology. You will have the opportunity to handle and use the various devices within the classroom setting. You can (b)(7)(E) This practice time enables you to take full advantage of practical application lab that follows. This lab will allow you to use the equipment in simulated field conditions.

The following technical surveillance equipment is available for you to practice.

(b)(7)(E)

Practice
You will be working with the following technical surveillance equipment:
(b)(7)(E)

Each person in your group should complete the following tasks:
(b)(7)(E)

CONCLUSION

Summary of Main Ideas

Electronic surveillance is an essential tool in HSI's investigative activity. New developments in electronic technology will continue to enhance SAs' ability to conduct successful investigations.

Using this equipment requires specific guidelines regarding its use, procurement, and storage. The willful act of intercepting or attempting to intercept any wire or oral non-consensual communications without a court order can result in a penalty with a maximum of 5 years of imprisonment (18 USC 2511(1)).

The lesson reviewed telephone intercepts, the seven sensitive investigative categories requiring special approvals, and the electronic equipment used.

SAs who anticipate using electronic surveillance equipment should seek assistance from the Technical Enforcement Officer (TEO) or Designated Technical Agent (DTA). Make contact with them as early in the planning stage as possible.

Integration

The ability to obtain information directly from a subject can augment an investigation or even take it in completely new directions. Choosing when and where to use electronic surveillance is an invaluable investigative strategy

Objectives

This lesson concentrated on consensual monitoring. The lesson focused on:

- Distinguishing between all-parties consent, consensual and non-consensual monitoring.
- Determining Department of Justice and HSI policies and procedures for the interception and/or recording of consensually monitored verbal communications.
- Identifying HSI policies and procedures for the issuance and control of electronic surveillance equipment and evidence.
- Using basic functions of selected electronic surveillance equipment, (b)(7)(E) (b)(7)(E)

Motivation

This lesson focused on the fundamental aspects of electronic surveillance, specifically the differences between consensual and non-consensual monitoring. It covered the basics of selecting proper electronic surveillance equipment, conducting function checks, and use of the equipment. The Technical Operations Handbook provides guidance on the policies and procedures associated with using this equipment.

Test or Final Activity

The preparation for planning, testing, and using monitoring equipment will be based on performance during Practice Exercise 1.

The test for demonstrating the ability to prepare for and conduct an electronic surveillance occurs during a Practical Exercise.