Forging a New Legacy

Homeland Security Investigations Electronic Surveillance Training Program (ICE-SAT) ICE Academy
Terminal Performance Objective

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

- Distinguish between all-parties consent, consensual and non-consensual monitoring.
- Determine DOJ, DHS and HSI policies and procedures for the interception and/or recording of consensually monitored verbal communications.
- Identify HSI policies and procedures for issuance and control of electronic surveillance equipment and evidence.
- Use basic functions of selected electronic surveillance equipment, including covert. 
Review of the Past

Main Ideas

- Primary focus – various types of electronic surveillance equipment, specifically basic operation of surveillance equipment. Applications in the investigation of criminal activities.
Homeland Security Investigations (HSI)

Agenda

- Use the Technical Operations Handbook as guide
- Areas that may result in procedural or legal errors
- Consensual and non-consensual monitoring
- DOJ and HSI policies and procedures
- Basic function/operation of surveillance equipment
- Applications in the investigation of criminal activities
- Demonstration of use of surveillance equipment
- Practice using surveillance equipment
Non-Consensual Monitoring

Willful intercept or attempt to intercept any wire or oral non-consensual communications without a court order – criminal offense

- Penalty – maximum 5 years of imprisonment

No parties to the conversation have consented to the monitoring – also referred to as:

- “Wiretap” “Title III intercept”
Consensual Monitoring

At least one party has consented; consenting party is directly or indirectly working for the Government – UC agent or informant

All party consent – recorded conversation

“Interception”/“monitoring” – aural acquisition by electronic, mechanical, or other
Establish Prior Consent

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

(b)(5), (b)(7)(E)
Consensual Monitoring Approval Process

Homeland Security Investigations (HSI)

Taking a closer look
Consensual Monitoring

- DOJ delegates authority to head of investigative agency or designee
- Agency supervises, monitors, tracks, and approves all consensual monitoring
- HSI Consensual Monitoring
  Requests/Notifications and Reports of Use – documented and approved using the ICM
- DOJ requires prior written approval for “Sensitive Categories”
Member of Congress, federal judge, member of Executive Branch at Executive Level IV or above

Governor, Lt. Governor, Attorney General of State, Judge/justice of highest court of any State/Territory

Member of Witness Security Program

Member of foreign country’s diplomatic corps

Party in custody of U.S. Marshal's Service or Bureau of Prisons

Attorney General (AG), Deputy AG, Associate AG, Assistant AG, or U.S. Attorney in investigation’s district
Consensual Monitoring

- Reason for Monitoring
- Offense — principal federal criminal statute involved
- Location of Monitoring — judicial district where it will occur
- AUSA Concurrence — Name, date, and time
- Request Period — 30 or 60 days for certified UC ops
- Identification of Consenting Party — LEO, CI, or Cooperating Individual
Homeland Security Investigations (HSI)

Consensual Monitoring

Recordings and Preambles

(b)(5), (b)(7)(E)
Homeland Security Investigations (HSI)

Telephone Intercepts
Homeland Security Investigations (HSI)

Electronic Surveillance Equipment

INCLUDE

DOES NOT INCLUDE

(b)(5), (b)(7)(E)
Homeland Security Investigations (HSI)

Technical Support for Criminal Investigations

**Designated Technical Agent (DTA)**
- SA who supports criminal investigations through electronic surveillance and techniques

**Technical Enforcement Officer (TEO)**
- Primary LEO who supports through use of electronic surveillance equipment and techniques. Primary responsibility is gathering of evidence in furtherance of criminal prosecutions
About Using Another Agency’s Equipment

(5), (7)(E)
Withheld pursuant to exemption
(b)(5); (b)(7)(E)
of the Freedom of Information and Privacy Act
Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act
Page 2150

Withheld pursuant to exemption

(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Planning the Operation
Page 2152

Withheld pursuant to exemption
(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Page 2153

Withheld pursuant to exemption

(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Page 2154

Withheld pursuant to exemption

(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Page 2155

Withheld pursuant to exemption

(b)(5) ; (b)(7)(E)

of the Freedom of Information and Privacy Act
Page 2156

Withheld pursuant to exemption

(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Withheld pursuant to exemption
(b)(5); (b)(7)(E)
of the Freedom of Information and Privacy Act
Discussion and Demonstration #2
Withheld pursuant to exemption
(b)(5); (b)(7)(E)

of the Freedom of Information and Privacy Act
Withheld pursuant to exemption
(b)(5) ; (b)(7)(E)
of the Freedom of Information and Privacy Act
Summary

• Electronic surveillance – essential investigative tool
  New electronic technology enhances SAs’ ability to conduct successful surveillances
  Specific guidelines – for use, procurement, storage
  Willful intercept of wire or oral non-consensual communications without court order = possible imprisonment
  Engage TEO/DTA early in planning stage
Protecting the Borders Against Illicit Trade, Travel, and Finance