

# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (7 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (8 of 8)

(b)(7)(E)





# Homeland Security Investigations (HSI)

## Recruiting – Basic Marketing

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Recruiting – Basic Sales

How is motivation used to recruit and manage CIs?

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Demonstration #1: Recruiting Pool

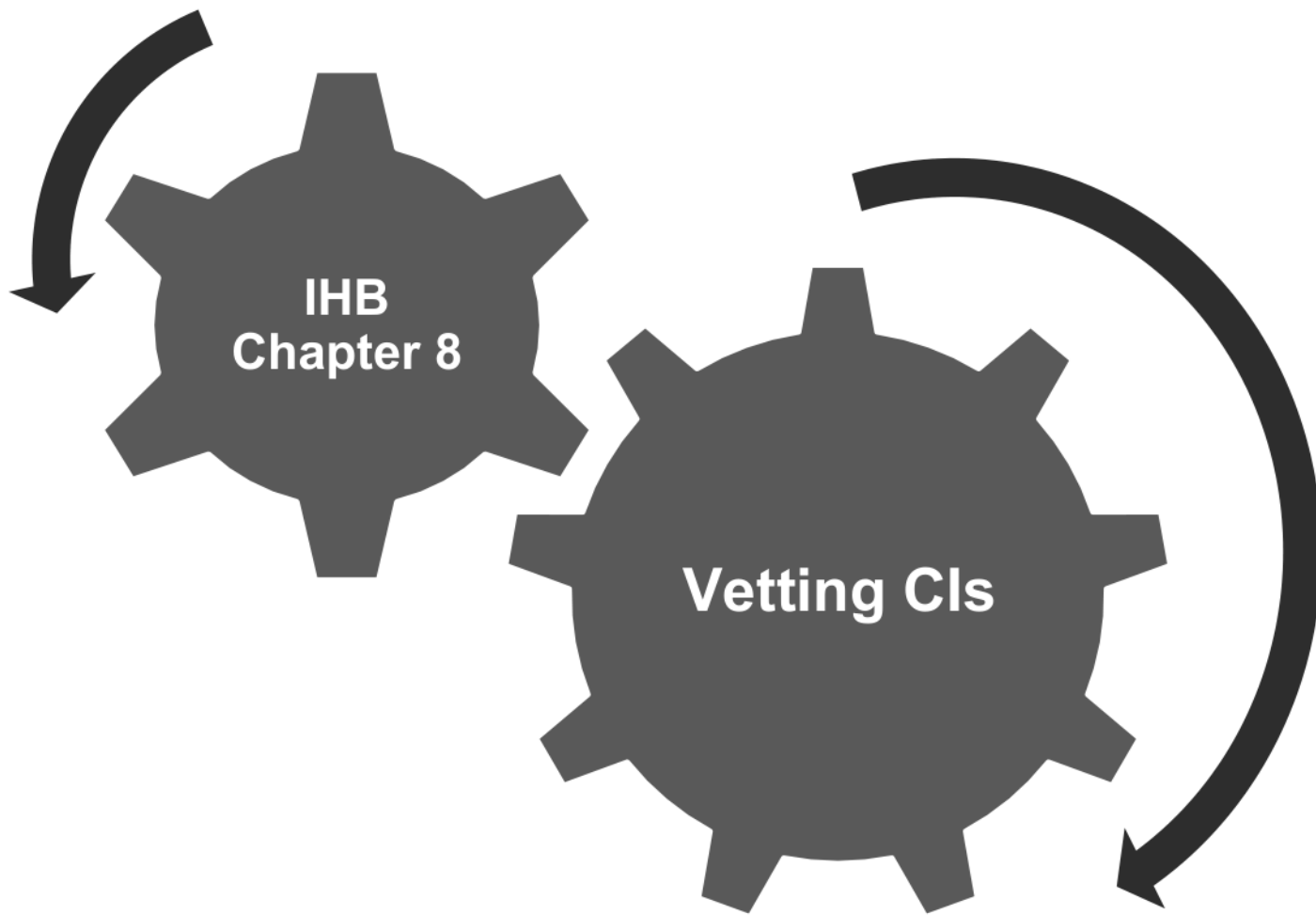
Your thoughts on the following persons as potential CIs? Why?

(b)(7)(E)

Demonstration #1 scenario is in the Student Guide



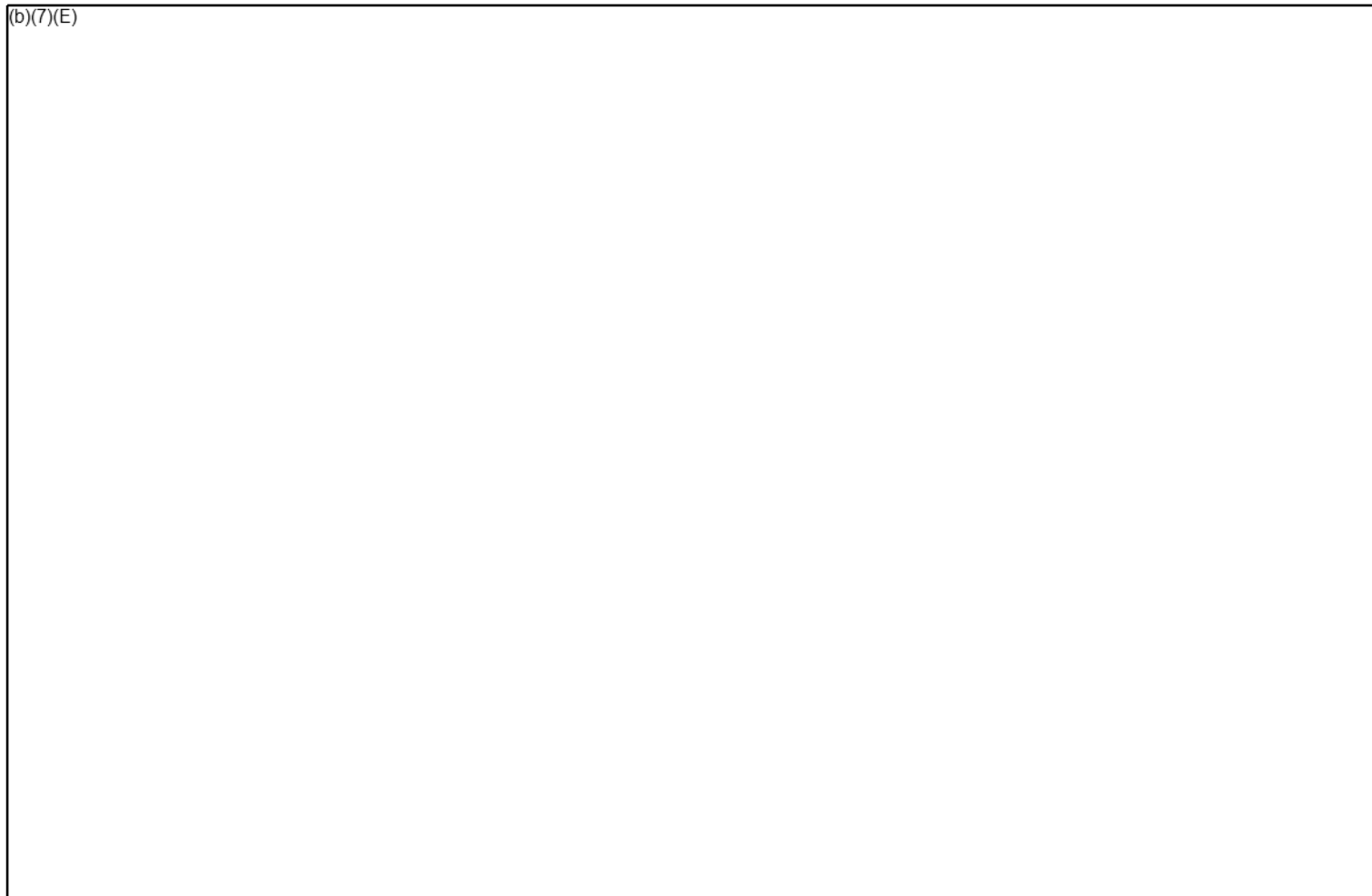
# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## Vetting a CI

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Assessment of CI's abilities

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Evaluation of Suitability (1 of 2)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Evaluation of Suitability (2 of 2)

(b)(7)(E)





# Homeland Security Investigations (HSI)

## Special Approval Requirements

**Coordination with other U.S. agencies, e.g.,  
DOJ – for uses of:**

(b)(7)(E)

# Homeland Security Investigations (HSI)

## DAD/ISD Approvals

SA must get written approval to use any of the following individuals as a CI:

(b)(7)(E)

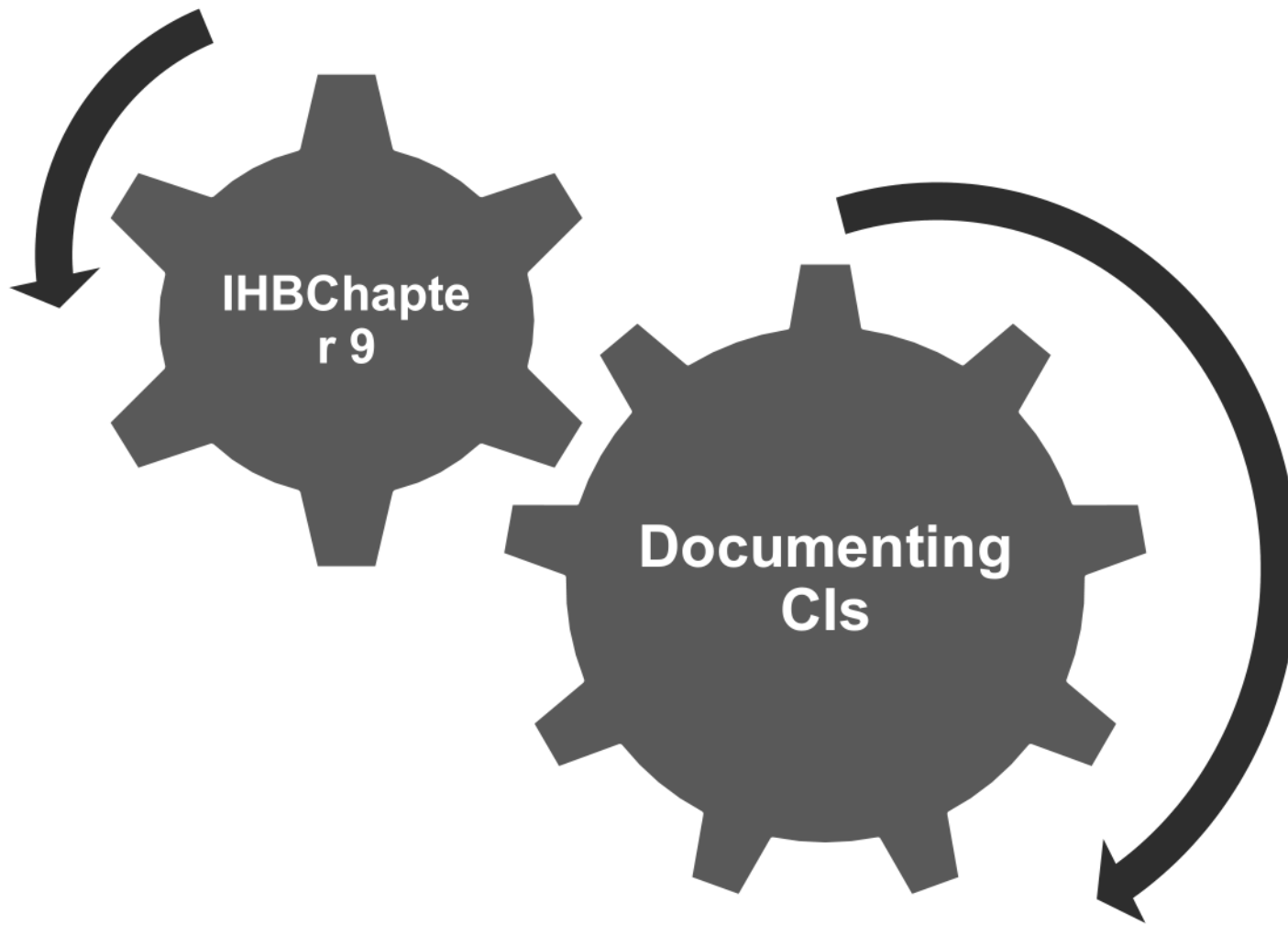
# Homeland Security Investigations (HSI)

## SAC Approvals

**SA must get written approval prior to using any of the following individuals as a CI:**

(b)(7)(E)

# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## CI Files

Created for each individual CI by the control agent

Maintained

(b)(7)(E)

(b)(7)(E)

CI number assigned when file complete

The "Confidential Informant Activation/Reactivation Checklist" is used to ensure that all required items are included in the CI file



# Homeland Security Investigations (HSI)

## Key CI File Forms

(b)(7)(E)

The image shows a large, empty rectangular area that has been redacted, indicated by the text "(b)(7)(E)" in the top-left corner. To the right of this main area is a vertical column of ten small, empty rectangular boxes, which likely represent a list or a set of checkboxes. The entire content is presented on a white background.





# CI Activation/ Reactivation Checklist

## CONFIDENTIAL INFORMANT ACTIVATION/REACTIVATION CHECKLIST

Date: \_\_\_\_\_

Control Agent: \_\_\_\_\_

Alternate Control Agent: \_\_\_\_\_

### Completed

(b)(7)(E)

### Special Authorizations

(b)(7)(E)

Control Agent's Signature: \_\_\_\_\_

Supervisory Review and Approval: \_\_\_\_\_

CI Number Assigned by the Field CI Program Administrator: \_\_\_\_\_



Page 2428

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2429

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

# Instructions to CI

## INSTRUCTIONS TO CONFIDENTIAL INFORMANT

These instructions are to be read to all individuals who are working as confidential informants. The reading of these instructions must be witnessed by the control agent and another law enforcement officer. These instructions must be signed and dated by the confidential informant, the control agent, and the witness. The confidential informant must initial each instruction.

- 1) \_\_\_\_ You are not an employee of U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI).
- 2) \_\_\_\_ You are not a law enforcement officer and will not represent yourself as a law enforcement officer to anyone.
- 3) \_\_\_\_ You are not permitted to violate any laws and could be prosecuted for any unauthorized criminal conduct in which you have previously engaged or in which you may engage in the future.
- 4) \_\_\_\_ Your status and documentation as a confidential informant do not convey any authority, statutory or otherwise, to carry a firearm or other weapon. When participating in authorized activity, you will not carry a firearm or other weapon, even if state laws or regulations allow you to carry one.
- 5) \_\_\_\_ You are not permitted to possess contraband and/or evidence without the prior knowledge and consent of your control agent.
- 6) \_\_\_\_ You consent to a search of your person and the conveyance under your control before and after every controlled meeting, transfer of monetary instruments, purchase of contraband, or other enforcement activity.
- 7) \_\_\_\_ You are not to use your association with HSI to resolve personal matters.
- 8) \_\_\_\_ You will follow the directions and instructions of your control agent and/or alternate control agent at all times. You will not take or seek to take any independent action on behalf of the U.S. Government.
- 9) \_\_\_\_ You will be truthful at all times when providing information to HSI Special Agents. You may be required to submit to a psychophysiological detection of deception examination (formerly known as a polygraph examination or lie detector test) to verify your information.
- 10) \_\_\_\_ You will not deliberately entrap any individual who would not otherwise be predisposed to commit a crime.

- 11) \_\_\_\_ You are not to disclose that you provide a service to HSI without the approval of your control agent.
- 12) \_\_\_\_ The information you provide to HSI may be used in a criminal proceeding. HSI will use all lawful means to protect your identity, but cannot guarantee that it will not be divulged.
- 13) \_\_\_\_ If any immigration benefit has been or will be provided to you and/or members of your immediate family for your cooperation, such benefits will allow you to remain in the United States, its commonwealths, and/or its territories only as long as needed to assist HSI and under the terms and conditions set by HSI. Immigration benefits granted by HSI will be revoked upon completion of your assistance. Any permanent residency status will be granted only subject to existing laws, and nothing will prevent you from applying for an immigration benefit for which you are otherwise eligible.
- 14) \_\_\_\_ You understand that HSI has not made any promises to you regarding permanent immigration status for you or your family.
- 15) \_\_\_\_ Your assistance and statements to HSI are entirely voluntary.

By signing this agreement, I hereby state that I have read these instructions or have had them read to me and that I have understood the above conditions set out to me.

\_\_\_\_\_  
Signature (Assumed Name)  
(Signature exemplar contained in the CI file)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Special Agent's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Special Agent's Name

\_\_\_\_\_  
Witness' Signature

\_\_\_\_\_  
Date

Page 2431

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

# CI's Criminal History Check

## CONFIDENTIAL INFORMANT CRIMINAL HISTORY CHECK

Confidential Informant Number: \_\_\_\_\_

Control Agent: \_\_\_\_\_

Agencies Checked	Date Checked	Check One	
		Negative	Positive
(b)(7)(E)			

### Summary of Criminal History Checks

<u>Date of Arrest</u>	<u>Agency</u>	<u>Charge</u>	<u>Disposition</u>
Assistant Special Agent in Charge (or higher) Authorization on File:		Yes	No

Control Agent's Signature: \_\_\_\_\_ Date: \_\_\_\_\_

# CI's Emergency Contact Information

## CONFIDENTIAL INFORMANT'S EMERGENCY CONTACT INFORMATION

Date: \_\_\_\_\_

Confidential Informant (CI) Number: \_\_\_\_\_

Control Agent: \_\_\_\_\_

### Contact Information – Other than Confidential Informant's

Name: \_\_\_\_\_

Relationship to the CI: \_\_\_\_\_

Telephone(s): \_\_\_\_\_

Address: \_\_\_\_\_

\_\_\_\_\_

CI's Signature: \_\_\_\_\_

Special Agent's Signature: \_\_\_\_\_

Witness' Signature: \_\_\_\_\_



# Homeland Security Investigations (HSI)

## CI File Maintenance Requirements (1 of 2)

- Maintained for 5 years (b)(7)(E) CI  
numberControlling agent prepares a brief (b)(7)(E) ROI –

(b)(7)(E)



# Homeland Security Investigations (HSI)

## CI File Maintenance Requirements (2 of 2)

- (b)(7)(E)

# Homeland Security Investigations (HSI)

## Other common CI file forms/additions

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Other common CI file forms/additions (Cont'd)

(b)(7)(E)

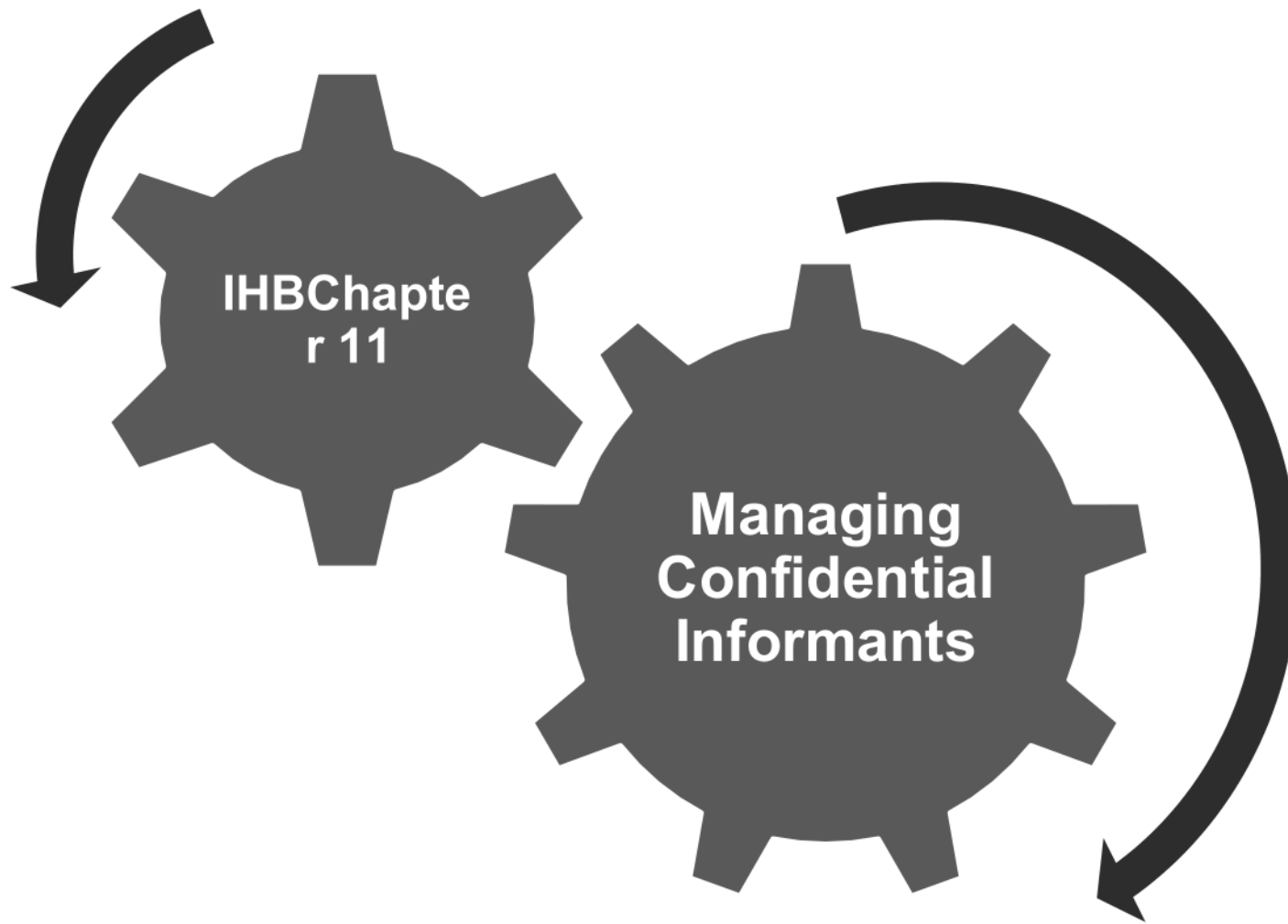
# Homeland Security Investigations (HSI)

## Demonstration #2: Complete a Source Card

(b)(7)(E)

Demonstration #2 scenario is in the Student Guide

# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## Prohibited Transactions and Relationships (1 of 2)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Prohibited Transactions and Relationships (2 of 2)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Meetings and Debriefings

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Documenting Information Received

Document all contact between CI and SA

Protects HSI, CI, and the integrity of the investigation

Document contact in a ROI

- Reference assigned CI number only
- Detail date, time, method of contact, individuals present, location, and information provided

Contact yields nothing – document in investigative notes

If CBP prepares a MOIR – place copy in source file

# Homeland Security Investigations (HSI)

## Demonstration #3: Instructions to the CI

(b)(7)(E)



Demonstration #3 scenario is in the Student Guide



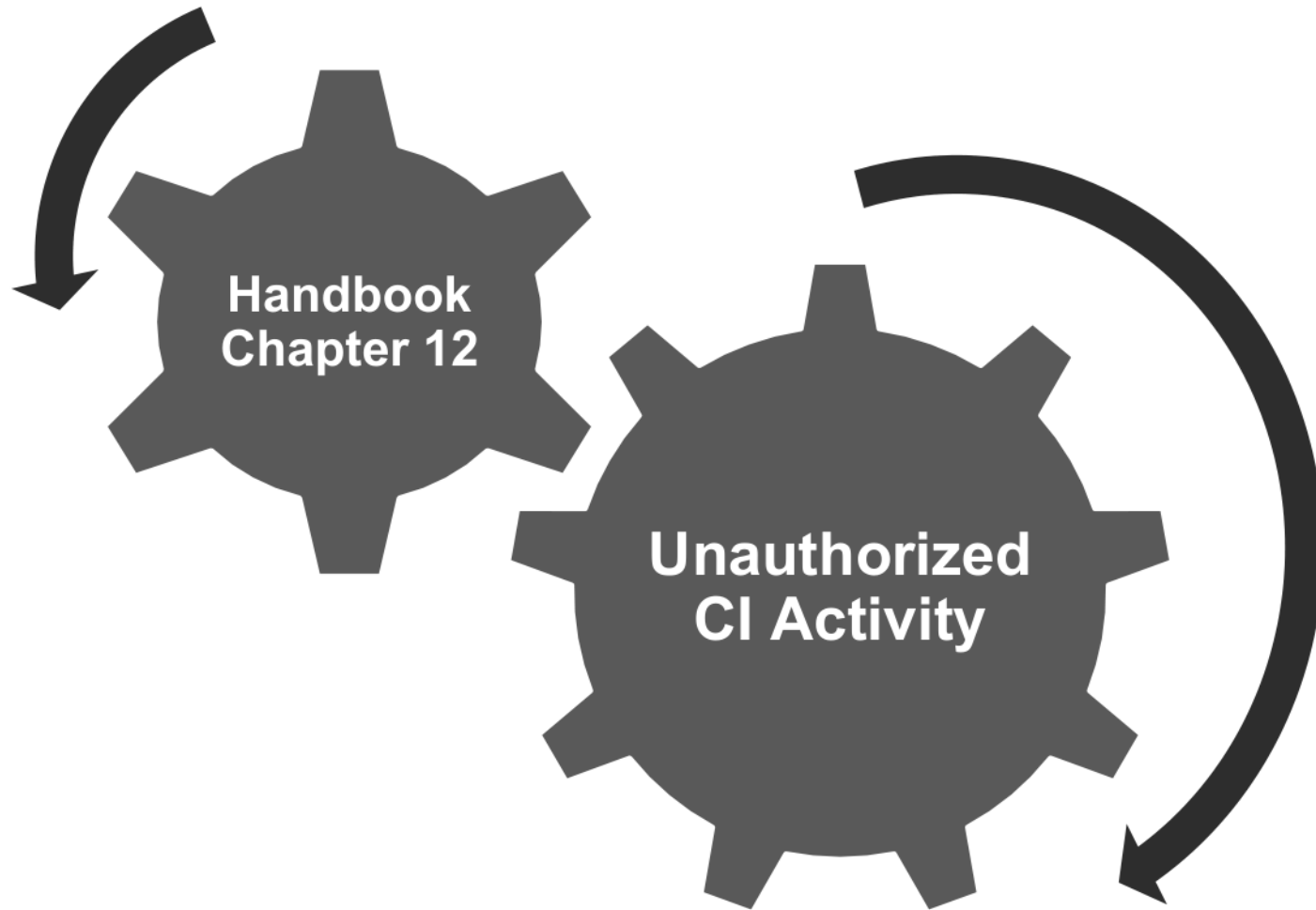
# Homeland Security Investigations (HSI)

## Working with Another LEA CI

(b)(7)(E)



# Homeland Security Investigations (HSI)



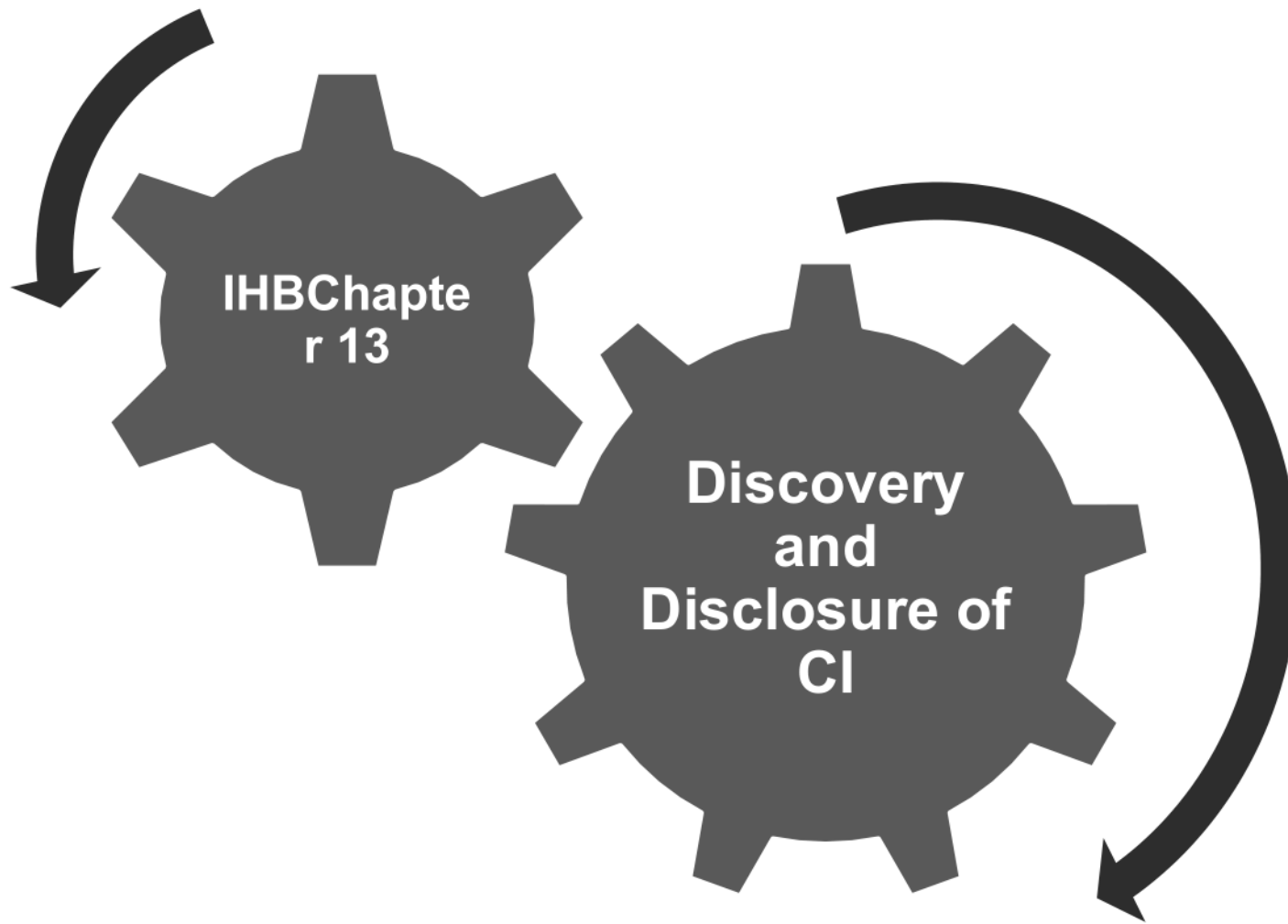
# Homeland Security Investigations (HSI)

## Unauthorized CI Activity

(b)(7)(E)



# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## Discovery, Disclosure and CIs

CIs have reasonable expectation of confidentiality and anonymity

### Giglio Doctrine

- Prosecution must provide defense with information affecting government witness' credibility
- Defense favors Rule 16 of the Federal Rules of Criminal Procedure, "Discovery and Inspections"

### Reasons for Disclosure

- Court Orders, Subpoenas
- CI or SA testimony
- Immigration proceedings

# Homeland Security Investigations (HSI)

## Protect CI Identity

to the Maximum Legal Extent

HSI policy: Disclosure requires EAD approval

- Official need-to-know required (except OPR & DHS OIG)
- Authorized for LEO safety and security

Investigative strategy

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Protect CI Identity (cont'd)

to the Maximum Legal Extent

CI file contents and testimony provided only with EAD, HSI written approval

CI file outside HSI provided via memo to DAD, ISD

Unauthorized disclosure via SAC memo to EAD

# Homeland Security Investigations (HSI)

## Procedures for Disclosure/Review of CI File

### Disclosure

- For judicial proceeding (criminal or civil):

(b)(7)(E)

(b)(7)(E)

- For subpoena, court order, other formal legal request:

(b)(7)(E)

### Review by AUSA, state/local prosecutor, or OPLA attorney

- HSI SA must witness review
- CI file shall not to be left unattended
- No copying files during review

# Homeland Security Investigations (HSI)

## CIs in Foreign Countries

Important to know rules to follow in foreign countries

Talk to international desk officer or appropriate attaché office for details, sign-offs and permissions

Documenting and reporting – document in same manner as a domestic CI

Arrests – notifications and timelines

CI foreign travel – Field office must obtain country clearance

# Homeland Security Investigations (HSI)

## CIs in Foreign Countries – Documenting

Important to know rules to follow in foreign countries

- A CI residing in and/or operating in a foreign country (foreign national or U.S. citizen) who will be documented and utilized as a CI shall be documented in the same manner as a domestic CI. Control Agent must complete a “Documentation of Confidential Informant Residing or Operating in a Foreign Country” memorandum when Domestic HSI office documents a foreign national residing and/or operating in a foreign country as a CI, and Domestic HSI office documents a U.S. citizen residing and/or operating in a foreign country



# Homeland Security Investigations (HSI)

## CIs in Foreign Countries

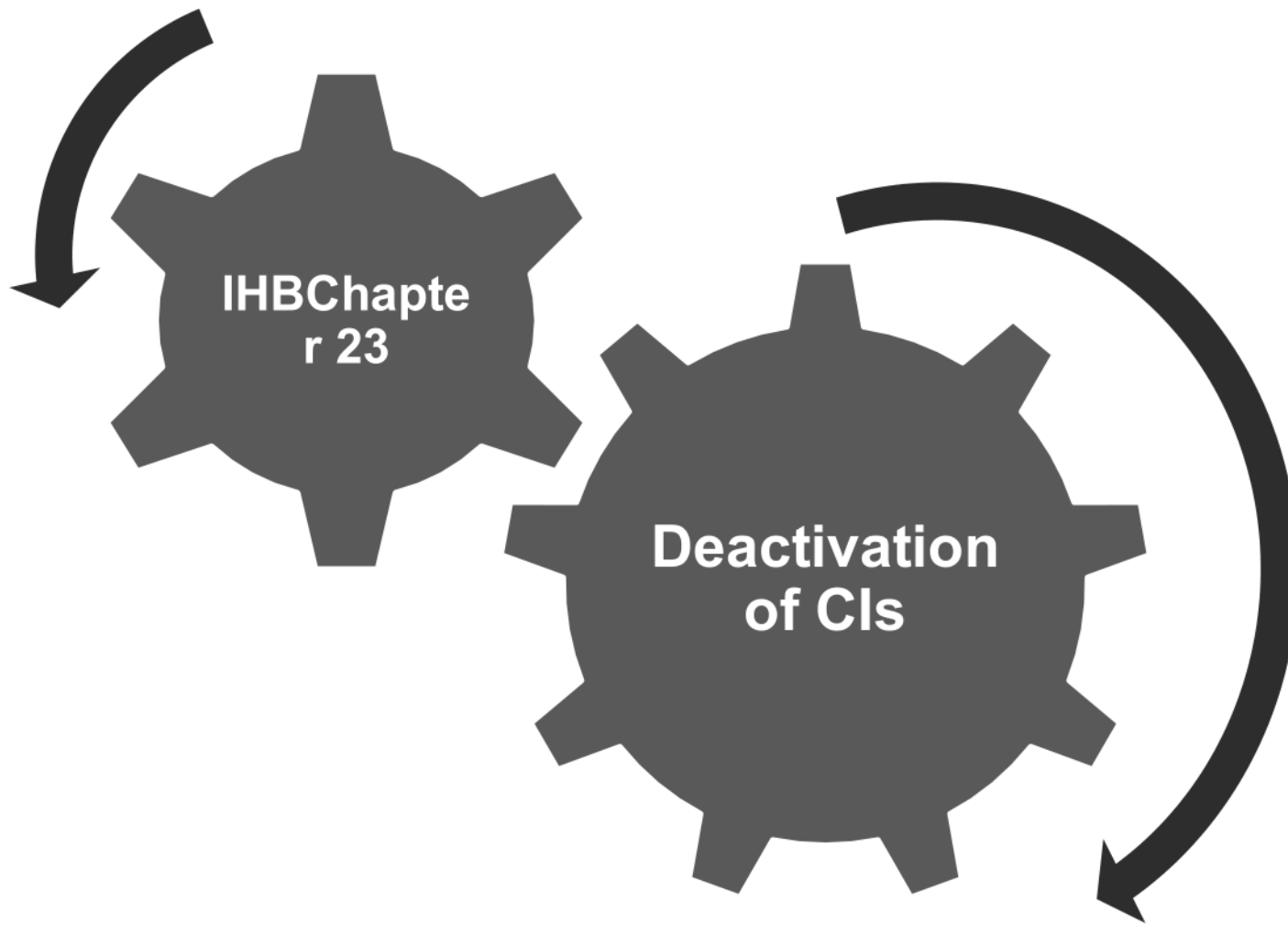
Title 21  
Investigations –  
agreement with  
DEA

- All investigative activity conducted under the provisions of Title 21 and involving controlled substances will be coordinated with DEA

CI activity in:

- Mexico: Agents should refer to the IHB section 14.4 for proper guidance reference the Brownsville/Merida MOU
- Canada: Check with Attaché office prior to CI activity for policy and guidelines (IHB 14.5)

# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

**A CI can be deactivated:**

(b)(7)(E)

# Homeland Security Investigations (HSI)

## CI Deactivation

Control agent will prepare a “Deactivation of Confidential Informant” memorandum for placement in the CI file

The notification of deactivation will be witnessed by at least one other LEO.

The FCPA will place a copy of the memo in the CI file and forward a copy to the DAD, ISU

The control agent should notify other investigative groups, HSI office or other agencies of the deactivation

If the CI is an alien, any temporary immigration benefits must be addressed



# Homeland Security Investigations (HSI)

## Deactivation for Cause

When a CI may be unreliable or undesirable

Follow all steps for general deactivation

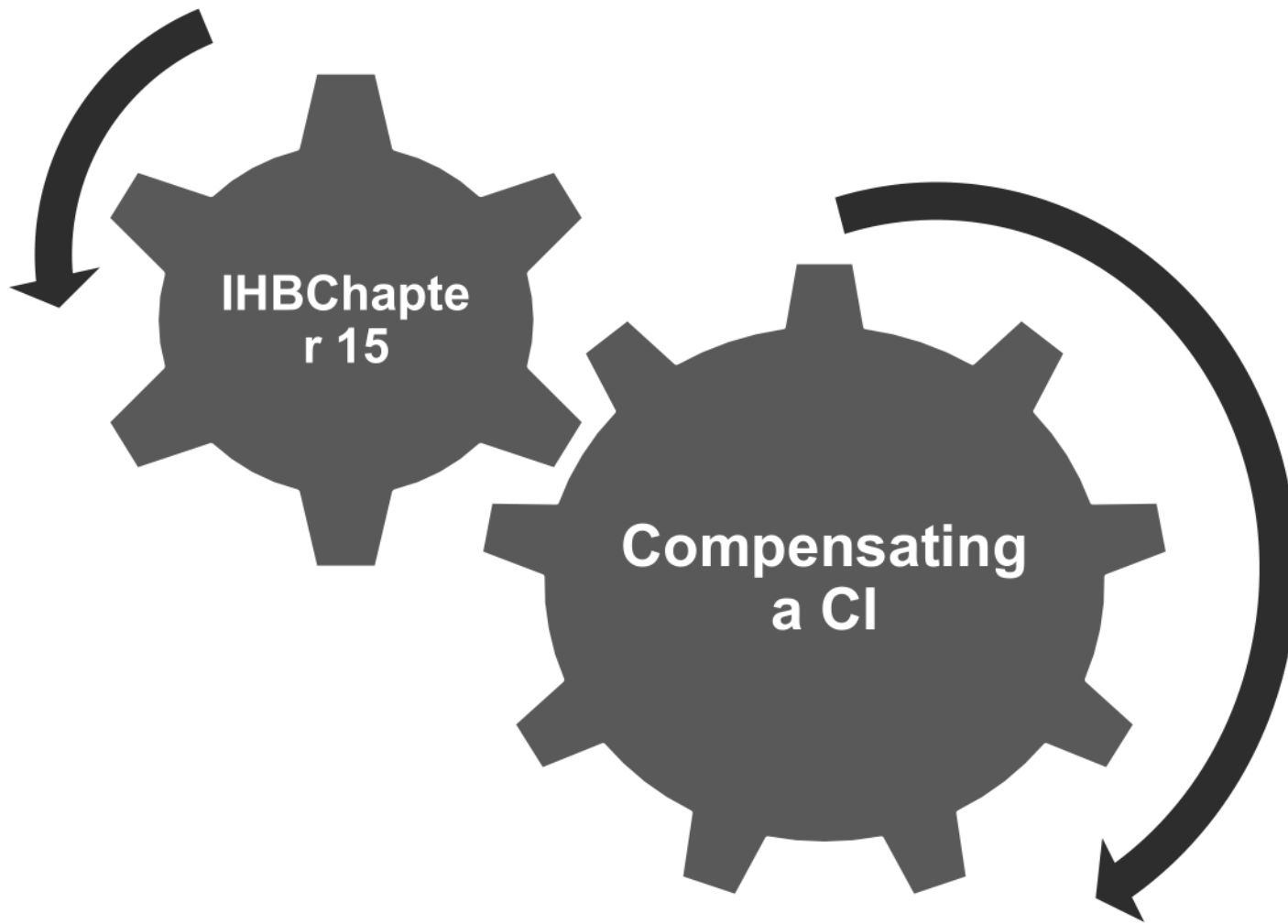
Document the reason for deactivation for cause in a memo to the DAD, ISU.

Notify appropriate prosecutors of deactivation

ISU will notify other HSI office in which the CI may have operated

ISU will also place the CI's name into (b)(7)(E) as a non-suspect

# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## CI Compensation (1 of 8)

There are a number of ways to compensate CIs

(b)(7)(E)

# Homeland Security Investigations (HSI)

## CI Compensation (2 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## CI Compensation (3 of 8)

### Commission

(b)(7)(E)

# Homeland Security Investigations (HSI)

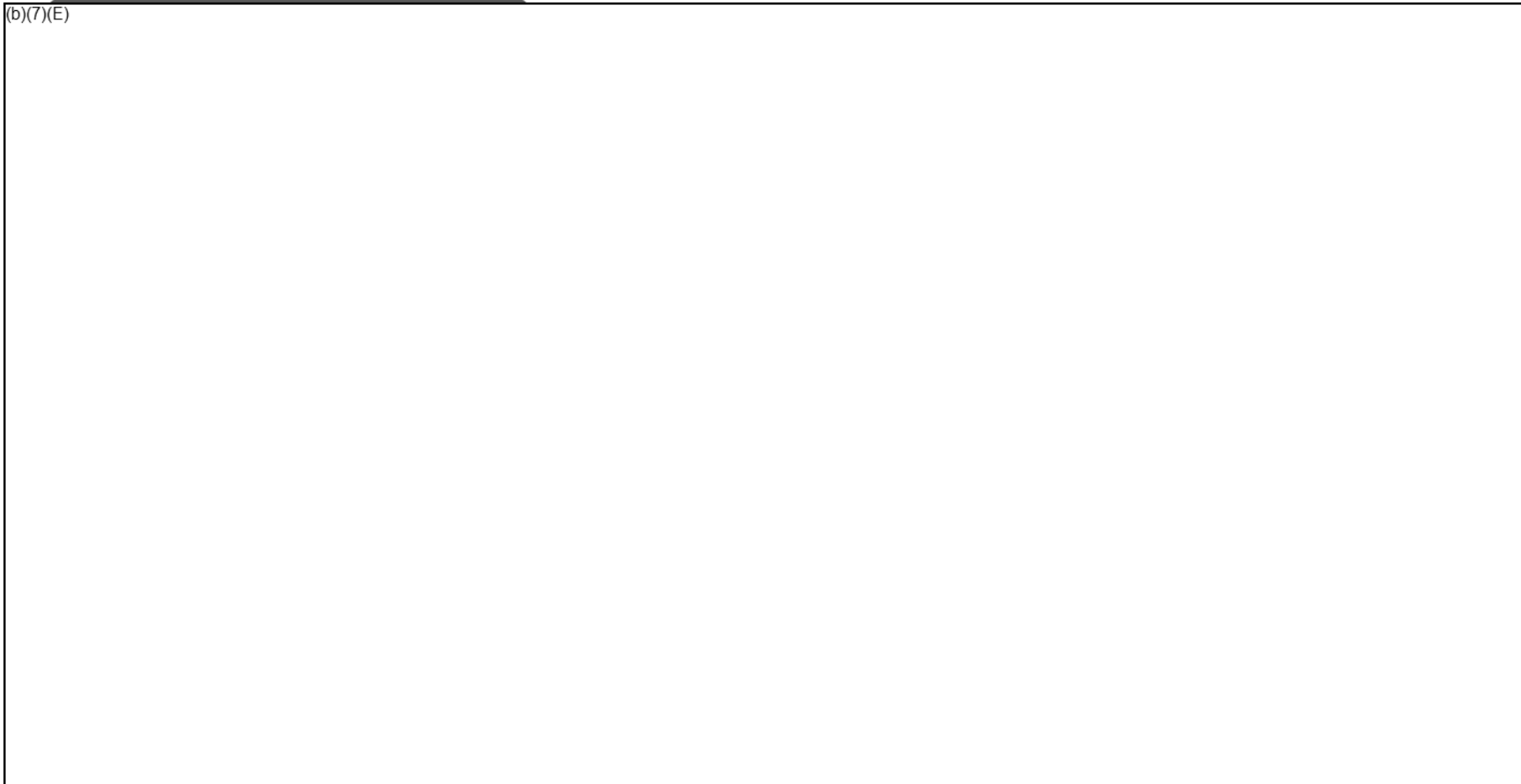
## CI Compensation (4 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## CI Compensation (5 of 8)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## CI Compensation (6 of 8)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## CI Compensation (7 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## CI Compensation (8 of 8)

Making the payment

Documenting the payment

(b)(7)(E)

# ICE Form 73-049

## 'Confidential Transaction Receipt'

Field Confidential Informant Program  
Administrators Signature

DEPARTMENT OF HOMELAND SECURITY  
U.S. Immigration and Customs Enforcement

### CONFIDENTIAL TRANSACTION RECEIPT

1. Control Number	2. ICE Office	3. Obligation No.	4. CUC Program Code	5. Date
6. Confidential Informant No. (If Applicable)	7. Case Number	8. Related FP&F Numbers		
<b>PAYMENT REQUEST</b>				
9. Type of Transaction	10. Funding Source (if other, indicate funding type in box 11)	11. If Other, Specify		
12. Enter Amount of Funds Requested (Type out)	13. Dollars		\$	
14. Assumed Name if CI or Real Name if Other				
15. Reason for Payment				
16. Requesting Agent (Name/Title/Office)		17. Date	18. Requesting Agent's Signature	
19. Final Approving Official (Name/Title/Office)		20. Date	21. Approving Official's Signature	
<b>PAYMENT BY DEBIT CARD/CHECK</b>				
22. Debit Card Doc Number	23. Check Number		24. Check Amount	
25. HQ/Local Approver		26. Date Approved		\$
27. Name/Title/Office of Agent Providing Funds/Check		Signature of Agent Providing Funds/Check		
28. Name/Title/Office of Agent Receiving Funds		Signature of Agent Receiving Funds		29. Date Funds Received
30. Name/Title/Office of Agent Making Payment		Signature of Agent Making Payment		31. Date Funds Paid
<b>TRANSFER OF FUNDS BY WIRE</b>				
32. Amount of Funds Received	TITLES AND SIGNATURES OF AGENTS RECEIVING FUNDS (Two Signatures Required)	33. Print Name/Title/Office	34. Signature	
\$		36. Print Name/Title/Office	37. Signature	
35. Date Funds Received				
<b>RETURN OF UNUSED FUNDS</b>				
38. Amount of Funds Returned	\$		39. Method of Return	40. Date of Return
41. Name/Title/Office of Agent Returning Funds		Signature of Agent Returning Funds		
42. Name/Title/Office of Witnessing Agent		Signature of Witnessing Agent		
<b>RECEIPT OF FUNDS</b>				
43. Received from U.S. Immigration and Customs Enforcement (ICE) for information provided to ICE in furtherance of an ICE investigation. Funds awarded for information provided to ICE are considered to be taxable income to the recipient and are required to be reported to the Internal Revenue Service.				
44. Amount of Funds Received				\$
45. Moleity Status <input type="checkbox"/> This payment is in lieu of Moleity <input type="checkbox"/> This payment is to be deducted from Moleity Initials of CI's Assumed Name: _____		46. Date Funds Received	47. Signature of Recipient (Assumed Name if CI or Real Name if Other)	
48. Signature of Witnessing Agent		49. Signature of Witnessing Agent		
50. Print Name/Title/Agency		51. Print Name/Title/Agency		

# Homeland Security Investigations (HSI)

## Judgment Criteria for Compensation (1 of 5)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Judgment Criteria for Compensation (2 of 5)

### Factors affecting amount of payment

(b)(7)(E)

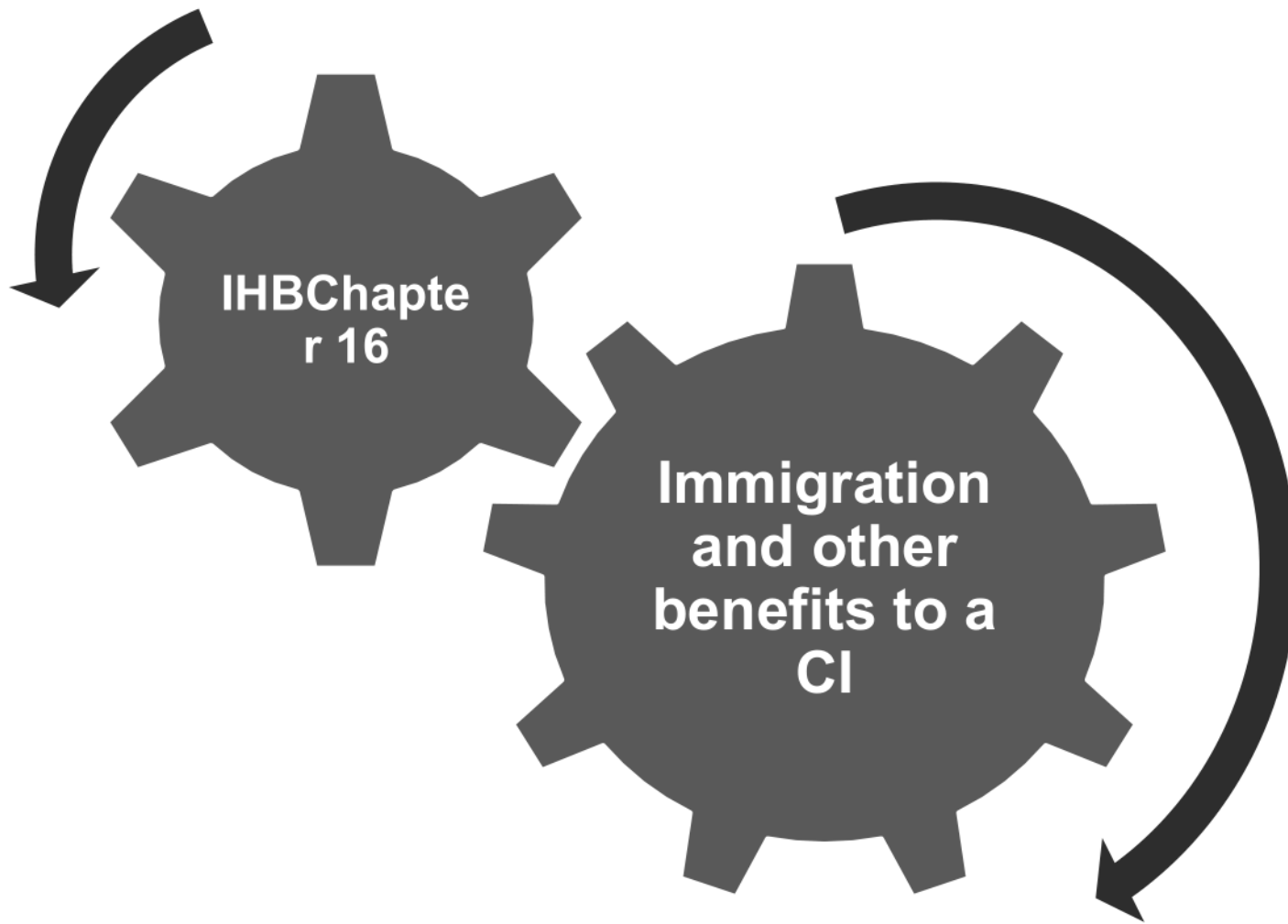
# Homeland Security Investigations (HSI)

## Judgment Criteria for Compensation (3 of 5)

### Funding Sources

(b)(7)(E)

# Homeland Security Investigations (HSI)



## Immigration and Other Benefits

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Immigration and Other Benefits (1 of 4)

(b)(7)(E)

# ICE Form 73-050

## 'Immigration Benefits Receipt'

Field Confidential Informant Program  
Administrator's Signature

DEPARTMENT OF HOMELAND SECURITY  
U.S. Immigration and Customs Enforcement

### IMMIGRATION BENEFITS RECEIPT

1. Control Number [redacted] - [redacted] - [redacted]		2. Confidential Informant No. SA - [redacted] - [redacted]	3. ICE Office [redacted]	4. CUC Program Code [redacted]	5. Case Number [redacted]
6. Date [redacted]	7a. Type of Immigration Benefit (if other, indicate benefit type in box 7b) [redacted]		7b. If other, specify [redacted]		
8. Immigration Benefit Recipient (if other, indicate relationship in box 9) [redacted]			9. If other, specify, e.g., SA-123-HQ (Relationship Type) [redacted]		
10. Period of Authorization for the benefit [redacted]			11. Assumed Name if CI or Real Name if Other [redacted]		
12. Reason for the Benefit [redacted]					
13. Requesting Agent (Name/Title/Office) [redacted]			14. Requesting Agent's Signature [redacted]		15. Date [redacted]
16. Approving Official (Name/Title/Office) [redacted]			17. Approving Official's Signature [redacted]		18. Date [redacted]
<b>RECEIPT OF IMMIGRATION BENEFITS</b>					
Received from U.S. Immigration and Customs Enforcement (ICE) the following immigration benefit for cooperation in the investigation of violations of laws enforced by ICE. Benefits provided by ICE are subject to all applicable laws, regulations, and policy and may be revoked at any time in accordance with the terms of the program under which the benefit was provided.					
19a. Type of Immigration Benefit (if other, indicate benefit type in next box) [redacted]			19b. If other, indicate benefit type [redacted]		
20. Immigration Benefit Recipient (if other, indicate relationship in the next box) [redacted]			21. If other, indicate relationship, e.g., SA-123-HQ (Relationship Type) [redacted]		
22. Assumed Name Signature of the CI [redacted]					23. Date Benefit Is Received [redacted]
<b>WITNESSING SIGNATURES</b>					
24. Print Name/Title/Agency [redacted]				25. Signature of Witness [redacted]	
26. Print Name/Title/Agency [redacted]				27. Signature of Witness [redacted]	

# Homeland Security Investigations (HSI)

## Immigration and Other Benefits (2 of 4)

### Approval and Documentation

- All requests for benefits require SAC approval
- Parole requests from ICE/HSI office in foreign countries require approval by respective HSI Attaché (ICE Form 73-050)

# Homeland Security Investigations (HSI)

## Immigration and Other Benefits (3 of 4)

### Parole/Significant Public Benefit Parole

- Allows temporary lawful presence in the U.S. for an alien in furtherance of investigation and/or prosecution
- Valid for one year (may be extended)
- Issued through the Parole and Law Enforcement Programs Unit
- Employment Authorization may also be requested

### Deferred Action

- Can postpone any 'action' from issuance of a NTA, effecting removal or effecting a reinstated order
- Valid for one year (may be extended)
- Issued locally by a SAC or designee
- Employment Authorization may also be requested

# Homeland Security Investigations (HSI)

## Practice #1: Recruit a CI

From your present or previous duty assignment....  
List three strategies for recruiting CIs in that location:

Practice #1 scenario is in the Student Guide

# Homeland Security Investigations (HSI)

## Practice #2: Complete a Source Card

(b)(7)(E)

Practice #2 scenario is in the Student Guide

# Homeland Security Investigations (HSI)

## Practice #3: Instructions to the CI

- (b)(7)(E)

Practice #3 scenario is in the Student Guide

# Homeland Security Investigations (HSI)

## Summary

- CIs Important to the HSI mission Potential threat to integrity of investigations and safety SAs cultivate and recruit CIs Extensive documentation & approval requirements Various methods of compensation Sources for guidance and information HSI Informants Handbook Seasoned SAs





Protecting the Borders Against Illicit Trade, Travel, and Finance

# **US Immigration and Customs Enforcement OFFICE OF TRAINING AND DEVELOPMENT**

## **ICE Academy**



## **CONFIDENTIAL INFORMANTS 11200**

### **Student Guide**

### **HSI Special Agent Training**

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). This contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, to anyone outside the ICE Academy, or to other personnel who do not have a valid "need-to-know" without prior approval of the ICE Office of Training and Development Assistant Director or his designee.



## Confidential Informants

### Motivation

Most significant investigations have one thing in common – informants. Informants are an extremely valuable tool to the HSI law enforcement mission and contribute significantly to our success. A good informant(s) can make or break an Agent's career and is one of the most important parts of becoming a good Agent.

Confidential Informants can be the eyes and ears in places that would otherwise be inaccessible to an HSI Special Agent. CIs can help agents build a sound investigation; however, these valuable tools can quickly become a double-edged sword: their self-interests often misalign with the Special Agent or HSI mission. An Agent's efforts, reputation, and investigation(s) may suffer if the CI's conduct or actions are inappropriate. Informant issues have been a primary factor in numerous Agent disciplinary actions and dismissals.

Based on experience, HSI has a detailed and extensive approval and review process for using Confidential Informants. The process serves to protect SAs, their cases and the Agency. At times, the process will seem aggravating –particularly when it slows down efforts in building the case. The process is in place to protect SAs and the Agency from possible public embarrassment, physical harm, or litigation.

### Objectives

#### Terminal Performance Objective (TPO)

**Conditions:** Given a set of case-related facts and a designated interaction with a potential Confidential Informant (CI),  
**Behavior:** follow the policies and procedures that the HSI Special Agent must accomplish  
**Criterion:** to successfully recruit, document, and compensate CIs according to the HSI Informants Handbook.

#### Enabling Performance Objectives (EPOs)

**EPO #1:** Discuss the primary considerations and strategies involved with the recruitment/cultivation of Confidential Informants (CIs).  
**EPO #2:** Describe the management of HSI Confidential Informants.  
**EPO #3:** Determine CI File maintenance requirements.  
**EPO #4:** Discuss options for compensating CIs.



## Review of the Past

During CITP training, students learned about working with Confidential Informants. CIs can be extremely valuable to investigations. While it is well known that CIs are important to the mission of HSI and have definitely contributed significantly to its success, the facts also set forth that CIs can often pose a potential threat to the integrity of investigations and to the safety of everyone involved. Failure to understand this fact is what, often times, leads to problems.

You also learned about Rule 16 of the Federal Rules of Criminal Procedure, “Discovery and Inspection” in legal training.

## Advance Organizer of Main Ideas

You are going to learn about using CIs in the context of Homeland Security Investigations. The objective is to lessen the occurrences of adverse CI interactions by providing you with the tools that will:

- more clearly define an informant or potential informant
- help you minimize the risk involved when interacting with CIs
- help you locate and adhere to the strict policies established in the HSI Informants Handbook – contains instruction and guidance to help ensure uniformity and operational consistency among all HSI field offices – found on HSI NET

*Note: Although the recurring term used in this lesson is “Confidential Informants” (CI), all policies and procedures discussed also apply to cooperating individuals (CIDs) unless otherwise noted.*

## Agenda

In order to meet our objectives in this lesson, we will:

- Discuss the primary considerations and strategies for recruiting and cultivating Confidential Informants.
- Describe the management of HSI Confidential Informants.
- Determine CI File maintenance requirements.
- Discuss options for compensating CIs.



## INSTRUCTION

### Explanation

**A. EPO #1: Discuss the primary considerations and strategies involved with the recruitment/cultivation of Confidential Informants.**

1. Confidential Informants

- a. The cultivation of informants and cooperators by HSI has contributed significantly to the success of the law enforcement mission.
- b. Due to the unpredictability of human behavior:

(b)(7)(E)

2. What or who is a source of information?

- a. SOIs and CIs are important to HSI's law enforcement mission and have contributed significantly to its success.

3. Categories of sources

a. Cooperating Defendant (CD):

- 1)
- 2)
- 3)

(b)(7)(E)

b. Confidential Informant (CI):

- 1)
- 2)
- 3)

(b)(7)(E)

c. Source of information (SOI):

- 1)
- 2)

(b)(7)(E)



3) (b)(7)(E)

d. (b)(7)(E)

**Notes:**

- 4. Who controls and directs sources?
  - a. HSI Special Agent acts as “Control Agent” (has the primary contact with a given CI).
  - b. Other ICE/HSI employees can cultivate and develop informants, but only Special Agents can document and control CIs.
  - c. HSI Task Force Officers (TFOs) can act as “alternate” (backup) control agent.

5. Categories of prospective informants/sources

a. (b)(7)(E)

Page 2490

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2491

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2492

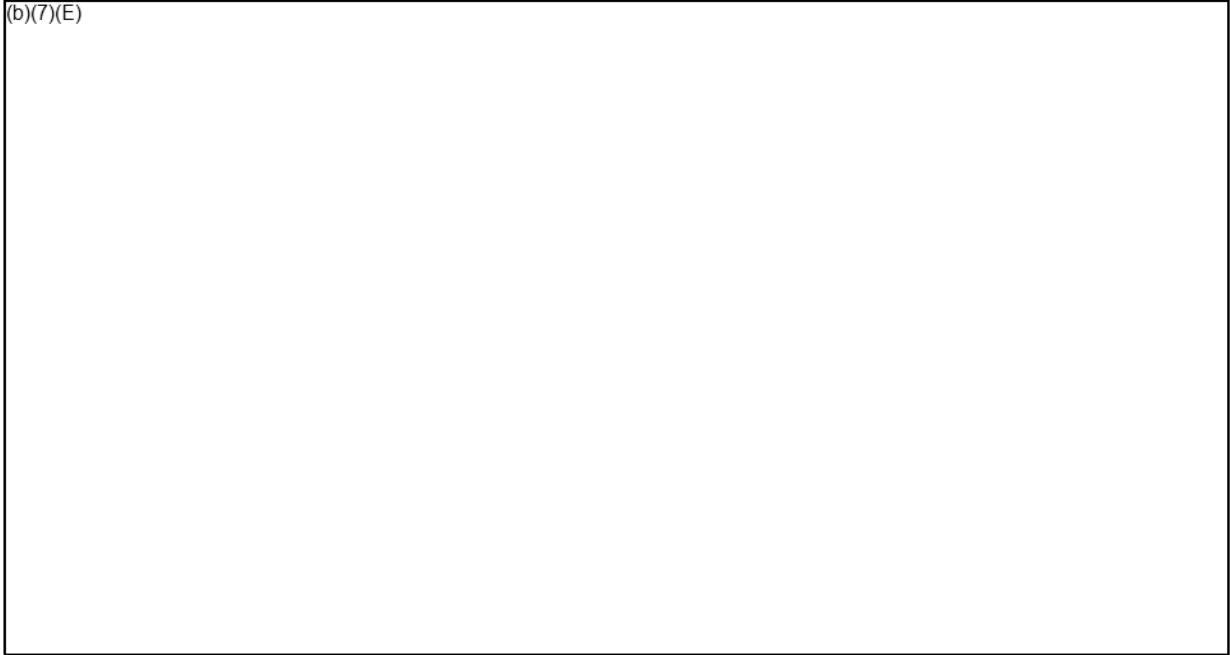
Withheld pursuant to exemption

(b)(7)(E)

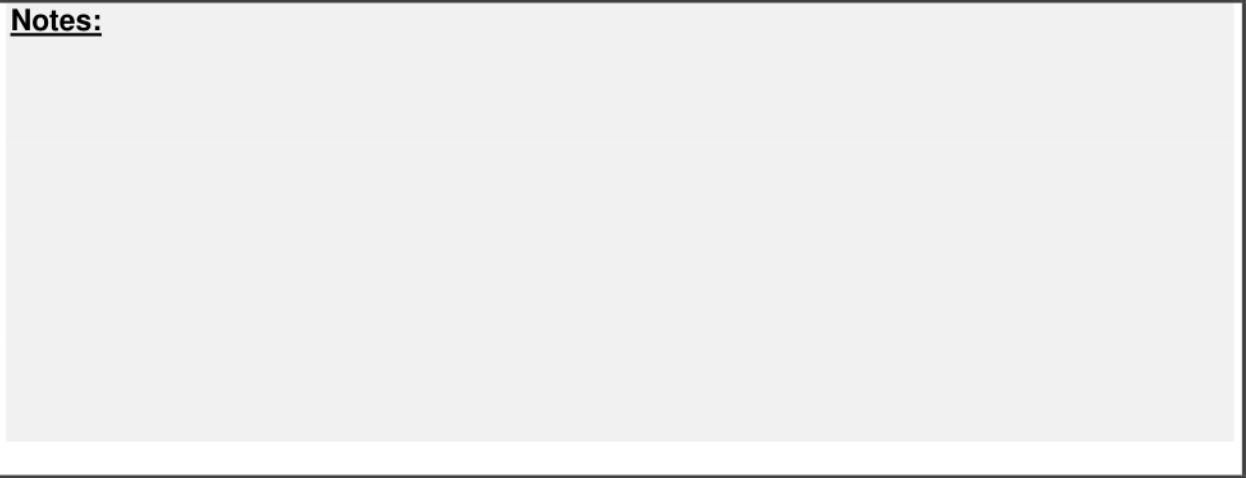
of the Freedom of Information and Privacy Act



(b)(7)(E)

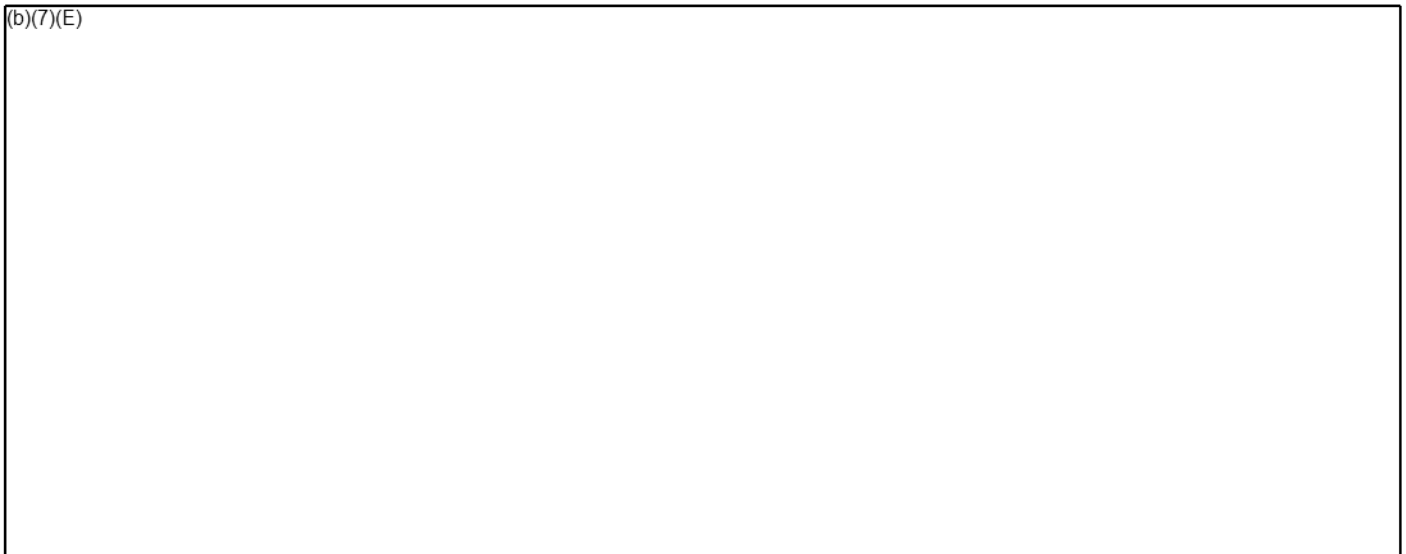


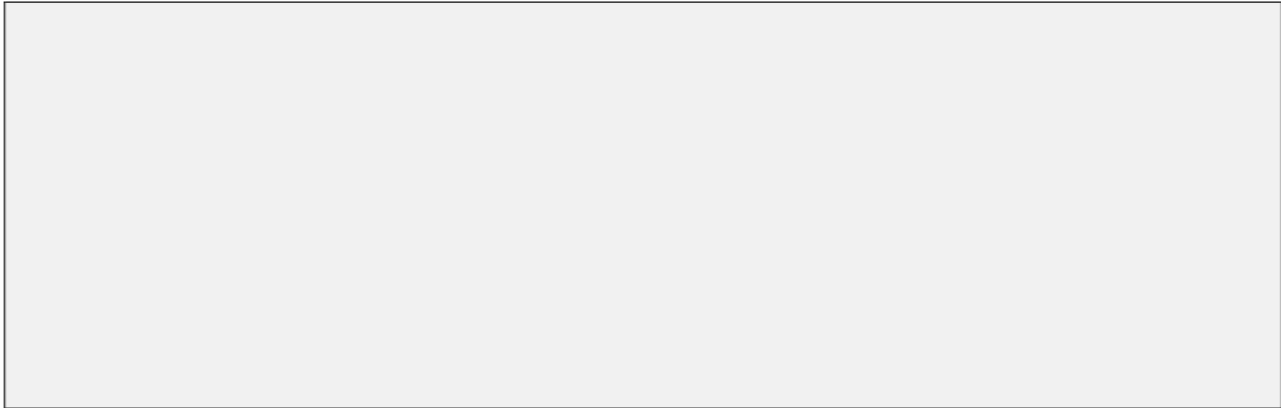
**Notes:**



**Demonstration #1 – Recruiting Pool**

(b)(7)(E)



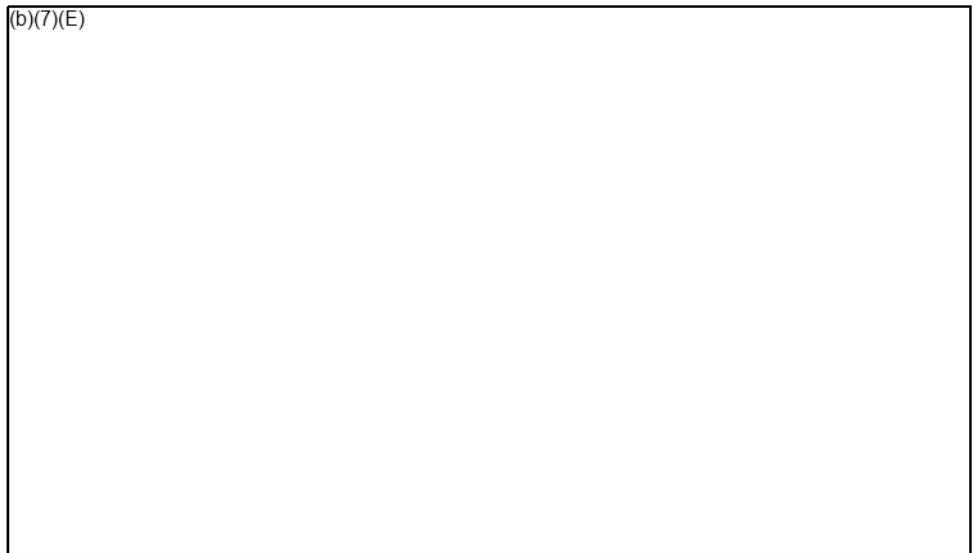


**B. EPO #2: Describe the management of HSI Confidential Informants.**

1. Vetting CIs (*Chapter 8*)

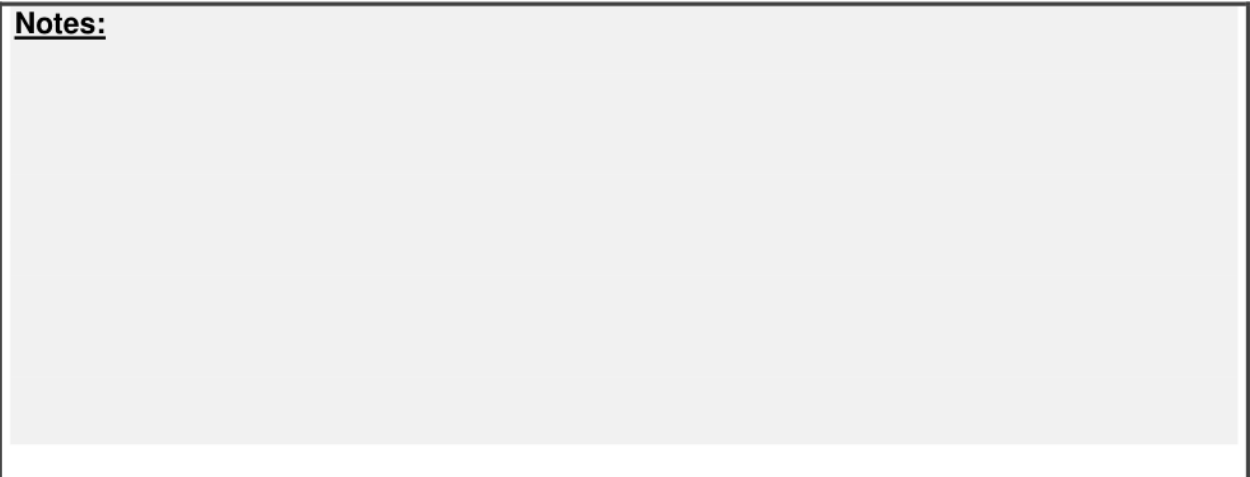
a. Assessment of CI's abilities (*Section 8.1*)

- 1)
- 2)
- 3)
- 4)



- 5)
- 6)
- 7)

**Notes:**





- b. Evaluation of suitability – GS and HSI SA must conduct initial evaluation in person and annually thereafter. Factors for determining CI suitability include:

(b)(7)(E)



(b)(7)(E)

**Notes:**

- c. Special approval requirements – Coordination with other U.S. agencies, for example, DOJ – for uses of:

- 1)
- 2)
- 3)

(b)(7)(E)



- b) (b)(5)
- c)
- d)
- e)
- f)

4) State/local Prisoners

- a) OEO approval is not required.
- b) The request must be approved by the DAD, ISD, and by the AUSA and/or the state or local prosecutor, as appropriate.

5) DAD/ISD approvals (Deputy Assistant Director, Investigative Services Division)

SAs must receive written approval from the DAD, ISD, prior to utilizing any of the following individuals as a CI:

- a) (b)(7)(E)
- b)
- c)
- d)
- e)
- f)

6) SAC Approvals

SAs must receive written approval from the SAC prior to utilizing any of the following individuals as a CI. A memorandum containing justification and approval of the SAC must be obtained and placed in the CI file prior to utilizing the CI.

- a) (b)(7)(E)
- b)

Page 2498

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



2. Documenting CIs (*Chapter 9*)

When an SA identifies an individual who meets the criteria for becoming a productive CI, the SA must document that individual in accordance with the guidelines provided in the Informant Handbook.

a. CI Files

- 1) Only SAs are authorized to document informants.
- 2) Control Agent creates CI File.

(b)(7)(E)

3) Key CI File Forms

- a)
- b)
  
- c)
- d)
  
- e)
- f)
- g)
  
- h)
  
- i)

(b)(7)(E)

The Confidential Informant File Checklist can be used to ensure that all required items are included in the CI file (*Appendix B*).





**C. EPO #3: Determine CI File maintenance requirements.**

The CI File is subject to frequent management reviews and auditing to ensure the integrity of the CI program, so it is very important for consistency in the placement of documents within the CI File. Also, CI Files are subject to the office self-inspection process (SIP) which identifies non-compliance issues to HQ. Non-compliance reflects poorly on management—from first- and second-level office management to the SAC.

1. CI File
  - a. Maintenance/Security: maintain for 5 years in originating office
  - b. Access Control

2. CI number

- a. (b)(7)(E)
- b.
- c.
- d.
- e.
- f.

3. Complete required card and all forms.

**Notes:**

Page 2501

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

g.

h.

i.

j.

k.

l.

**Notes:**

**Demonstration #2 – Complete a Source Card**

Complete a Source Card for the CI selected in Demonstration #1. Use the electronic form, Confidential Informant Documentation, ICE Form 73-045.

- (b)(7)(E)



(b)(7)(E)

- 

6. Managing Confidential Informants (*Chapter 11*)

a. Prohibited Transactions and Relationships

1)

2)

3)

4)

5)

6)

7)

(b)(7)(E)

Page 2504

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



### Demonstration #3 – Instructions to the CI

(b)(7)(E)

7. Working with Another LEA CI

- a.
- b.
- c.
- d.

(b)(7)(E)

8. Unauthorized activity (*Chapter 12*)

- a.
- b.
- c.

(b)(7)(E)



- d. (b)(7)(E)
- e.
- f.
- g.
- h.

**Notes:**

- 9. Discovery and Disclosure of CI (*Chapter 13*)
  - a. CIs have reasonable expectation of confidentiality and anonymity.
  - b. Giglio Doctrine:
    - 1) Prosecution must provide defense with information affecting a government witness' credibility, including a summary of payments to the CI specific to the prosecution in which CI will testify.



- 2) Defense usually attempts to obtain CI info under Rule 16 of the Federal Rules of Criminal Procedure, "Discovery and Inspection."

c. Reasons for Disclosure

- 1) Court Orders
- 2) Subpoenas
- 3) CI or SA testimony
- 4) Immigration proceedings

d. Protect CI identity to the maximum extent of the law

- 1) Disclosure requires EAD, HSI approval.

(b)(7)(E)

- 2) Investigative strategy to protect

- a) (b)(7)(E)
- b)

- e. CI File contents and testimony provided only with EAD, HSI written approval.
- f. Disclosure of CI File outside HSI via memorandum to DAD, ISD.
- g. For unauthorized disclosure, SAC prepares and submits memorandum to EAD.

10. Procedures for Disclosure/Review of CI File

a. Disclosure

- 1) (b)(7)(E)
- 2)





b. Providing CI File for review

- 1) If AUSA, or state or local prosecutor (during judicial proceeding) or OPLA attorney (during immigration proceeding) requests to review CI's file:
  - a) HSI SA must witness review.
  - b) CI File shall not be left unattended. (Note: SAs are not authorized to allow state/local prosecutors of non-HSI cases to review CI File contents without prior consultation with ISU and (RDU).
  - c) AUSA, state/local prosecutors, or OPLA may not make copies of CI File during review.

**Notes:**

11. CIs in foreign countries

Rarely will new SAs develop CIs in foreign countries. However, if you are reporting to border locations must know the rules that CIs must follow while in foreign countries.

a. Important to know rules

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



(b)(7)(E)

b)

c)

4) CI foreign travel – Field office must obtain country clearance

b Documenting CIs in Foreign Countries

ClIs in foreign countries are documented in the same manner as a domestic CI.

- 1) A CI residing in and/or operating in a foreign country (foreign national or U.S. citizen) who will be documented and utilized as a CI shall be documented in the same manner as a domestic CI (as specified in Chapter 9 of the CI Handbook).
- 2) The control agent must complete a “Documentation of Confidential Informant Residing or Operating in a Foreign Country” memorandum (*Appendix H*) when:
  - a) Domestic HSI office documents a foreign national residing and/or operating in a foreign country as a CI, and
  - b) Domestic HSI office documents a U.S. citizen residing and/or operating in a foreign country.

c. ClIs in Foreign Countries

- 1) Title 21 Investigations
  - a) Pursuant Title 21 Investigations – agreement with DEA, all investigative activity conducted under the provisions of Title 21 and involving controlled substances will be coordinated with DEA.
- 2) CI activity in:
  - a) Mexico: refer to the IHB, *Section 14.4*) for proper guidance; reference the Brownsville/Merida MOU
  - b) Canada: check with Attaché office prior to CI activity for policy and guidelines; refer to the IHB, *Section 14.5*



**Notes:**

12. Deactivation of CIs (*Chapter 23*)

a. A CI can be deactivated for two reasons:

1)

(b)(7)(E)

2)

b. CI Deactivation Process

- 1) Control agent will prepare a "Deactivation of Confidential Informant" memorandum for placement in the CI file.
- 2) The notification of deactivation will be witnessed by at least one other LEO.
- 3) The FCPA will place a copy of the memo in the CI file and forward a copy to the DAD, ISU.
- 4) The control agent should notify other investigative groups, HSI office or other agencies of the deactivation.



- 5) If the CI is an alien, any temporary immigration benefits must be addressed.

c. Deactivation for Cause

- 1) Follow all steps for general deactivation.
- 2) Document the reason for deactivation for cause in a memo to the DAD, ISU.
- 3) Notify appropriate prosecutors of deactivation.
- 4) ISU will notify other HSI office in which the CI may have operated.
- 5) ISU will also place the CI's name into TECS ICM as a non-suspect.

**Notes:**

D.

(b)(7)(E)

Page 2512

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2513

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2514

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2515

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2516

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



## CONCLUSION

### Summary of Main Ideas

(b)(7)(E)

### Integration

Confidential Informants are an important part of an investigator's success. They can bring information to you, and they can help you legally confirm information to tighten your case. Their access to places and individuals that defy your best efforts can be invaluable.

(b)(7)(E)

Just about everywhere.

### Objectives

The objective in this class was to give you the tools that would lessen the occurrences of adverse outcome when interacting with a CI. You now can:

- Discuss the primary considerations and strategies involved with the recruitment/cultivation of Confidential Informants.
- Describe the management of HSI Confidential Informants.
- Determine CI File maintenance requirements.
- Discuss options for compensating CIs.



## Motivation

(b)(7)(E)

## Test or Final Activity

In several case scenarios that involve interactions with CIs, you must use the HSI Informants Handbook to determine:

- Appropriate actions to take
- Appropriate reports to file
- Proper documentation to complete
- Approval level required

You will demonstrate your ability to meet requirements contained in the HSI Informants Handbook in the context provided by the continuing case scenarios.

The test for the Confidential Informant lesson occurs during the Practical Exercise 1. Recruiting, interviewing, cultivating, and documenting CIs is part of a weighted final examination. Instructors will evaluate students by using a checklist to ensure that they adequately perform these important aspects of working with confidential informants.



**Appendix D**

**Instructions  
to  
Confidential Informant**

*Informants Handbook*  
August 2, 2012

*D-i*

*FOR OFFICIAL USE ONLY*  
*LAW ENFORCEMENT SENSITIVE*



## INSTRUCTIONS TO CONFIDENTIAL INFORMANT

These instructions are to be read to all individuals who are working as confidential informants. The reading of these instructions must be witnessed by the control agent and another law enforcement officer. These instructions must be signed and dated by the confidential informant, the control agent, and the witness. The confidential informant must initial each instruction.

- 1)  You are not an employee of U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI).
- 2)  You are not a law enforcement officer and will not represent yourself as a law enforcement officer to anyone.
- 3)  You are not permitted to violate any laws and could be prosecuted for any unauthorized criminal conduct in which you have previously engaged or in which you may engage in the future.
- 4)  Your status and documentation as a confidential informant do not convey any authority, statutory or otherwise, to carry a firearm or other weapon. When participating in authorized activity, you will not carry a firearm or other weapon, even if state laws or regulations allow you to carry one.
- 5)  You are not permitted to possess contraband and/or evidence without the prior knowledge and consent of your control agent.
- 6)  You consent to a search of your person and the conveyance under your control before and after every controlled meeting, transfer of monetary instruments, purchase of contraband, or other enforcement activity.
- 7)  You are not to use your association with HSI to resolve personal matters.
- 8)  You will follow the directions and instructions of your control agent and/or alternate control agent at all times. You will not take or seek to take any independent action on behalf of the U.S. Government.
- 9)  You will be truthful at all times when providing information to HSI Special Agents. You may be required to submit to a psychophysiological detection of deception examination (formerly known as a polygraph examination or lie detector test) to verify your information.
- 10)  You will not deliberately entrap any individual who would not otherwise be predisposed to commit a crime.



- 11) \_\_\_\_\_ You are not to disclose that you provide a service to HSI without the approval of your control agent.
- 12) \_\_\_\_\_ The information you provide to HSI may be used in a criminal proceeding. HSI will use all lawful means to protect your identity, but cannot guarantee that it will not be divulged.
- 13) \_\_\_\_\_ If any immigration benefit has been or will be provided to you and/or members of your immediate family for your cooperation, such benefits will allow you to remain in the United States, its commonwealths, and/or its territories only as long as needed to assist HSI and under the terms and conditions set by HSI. Immigration benefits granted by HSI will be revoked upon completion of your assistance. Any permanent residency status will be granted only subject to existing laws, and nothing will prevent you from applying for an immigration benefit for which you are otherwise eligible.
- 14) \_\_\_\_\_ You understand that HSI has not made any promises to you regarding permanent immigration status for you or your family.
- 15) \_\_\_\_\_ Your assistance and statements to HSI are entirely voluntary.

By signing this agreement, I hereby state that I have read these instructions or have had them read to me and that I have understood the above conditions set out to me.

\_\_\_\_\_  
Signature (Assumed Name)  
(Signature exemplar contained in the CI file)

\_\_\_\_\_  
Date

\_\_\_\_\_  
Special Agent's Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Special Agent's Name

\_\_\_\_\_  
Witness' Signature

\_\_\_\_\_  
Date



DEPARTMENT OF HOMELAND SECURITY  
U.S. Immigration and Customs Enforcement  
**CONFIDENTIAL INFORMANT DOCUMENTATION**

1. NAME (LAST, First, Middle)		2. Alien Number A#		3. Confidential Informant Number	
4. Assumed Name		5. A/K/A		6. Case Number	
7. Address		8. City		9. State	
10. Zip Code	11. Country		12. Date of Birth		13. Place of Birth
14. Citizenship (List All)		15. Race		16. Hispanic	17. Sex
18. Height ft in	19. Weight lbs	20. Eye Color		21. Hair Color	
22. Social Security Number		23. Driver's License Number		24. State	
25. Scars/Marks/Tattoos				26. Immigration Benefits Required	
27. NCIC	28. TECS	29. Other Criminal History		30. SAC/HQ Approval Required	
31a. Approving Officer		32a. Reason Approval is Required		33a. Date of Approval	
31b. Approving Officer		32b. Reason Approval is Required		33b. Date of Approval	
31c. Approving Officer		32c. Reason Approval is Required		33c. Date of Approval	
34a. Motivation					
34b. Motivation					
34c. Motivation					
35. Program Area(s) (List All That Apply, e.g., Financial, Counter Proliferation Investigations)					
36. Languages Spoken			37. Special Certifications/Licenses/Expertise		
38. Notes					
39. Documented by Other Law Enforcement Agency or HSI Office (List All) (If HSI, Include CI Number) Agencies/Offices:					
40. Control Agent (Full Name) and Badge Number			41. Alternate Control Agent (Full Name) and Badge Number		
42. Control Agent's Signature			43. Alternate Control Agent's Signature		
44. Confidential Informant Documentation Type <input type="checkbox"/> INITIAL <input type="checkbox"/> AMENDED <input type="checkbox"/> REACTIVATION				45. Date of Initial Activation	
46. Group Supervisor's Printed Name, Badge Number, Signature, and Date				47. FCPA Review/Initial	

All boxes must be filled out. If not applicable, type "N/A".



A. Complete the Confidential Informant (CI) Documentation. **Do not save the completed CI Documentation on your computer.**

B. Print a copy of the completed CI Documentation, signing/initialing where required.

C. The Field Confidential Informant Program administrator (FCPA) will scan the signed copy and email it to the Undercover Operations Unit (UOU) File Custodian, using an email with delivery and read receipt to show that it was delivered to and received by UOU. NOTE: The scanned form must be sent as an encrypted attachment, with a password sent separately. (See the Department of Homeland Security "Handbook for Safeguarding Sensitive Personally Identifiable Information," dated March 2012 or as updated for instructions on how to encrypt the file.)

D. Print a copy of the delivery and read receipt, seal the CI Documentation in an envelope, and place them in the CI file.

E. Delete the scanned PDF from your hard drive.

**PLEASE NOTE THE FOLLOWING**

**Box 26:** If the CI requires any type of immigration benefits, check "Yes".

**Box 30:** If the use of this CI requires approval to use, check "Yes". See the following sections of the Homeland Security Investigations (HSI) Informants Handbook (HSI HB 12-03, dated August 2, 2012) for required approvals:

- 8.3 Department of Justice Office of Enforcement Operations Approval
- 8.4 Utilizing a State or Local Prisoner
- 8.5 Deputy Assistant Director, Investigative Services Division, Approval
- 8.6 Special Agent in Charge Approval
- 8.7 Confidential Informants with Criminal History

**Box 31a, b, and c:** Include the name of the HSI official or the name of the outside agency from which approval was obtained (e.g., DOJ, OEO).

**Box 32a, b, and c:** State the reason approval was required from the HSI official or outside agency named in boxes 31a, b, and c (e.g., CI with a criminal history, former Witness Security Program participant).

**Box 33a, b, and c:** Include the date on which the HSI official or outside agency granted approval.

**Box 38:** Include any other pertinent information not already stated on the CI Documentation.

**Box 39:** If the CI has been or is currently documented by another law enforcement agency or HSI office, check "Yes". Include the names of all the agencies or offices. If the CI is documented by another HSI office, also include the CI number.

**Box 40:** Include the full name and badge number of the control agent.

**Box 41:** Include the full name and badge number of the alternate control agent. Also note whether the alternate control agent is a Special Agent or a Task Force Officer.

**Box 44:** Check the appropriate box to show the type of CI documentation. There are three types:

- An initial CI documentation, which shows your office's documentation of a CI for the first time.
- An amended CI documentation, which shows any changes in the CI's information or change of the control agent or alternate control agent.
- A reactivation CI documentation, which is used to reactivate a CI previously deactivated in your office.

**Box 45:** If the CI documentation is an amended documentation or a reactivation, include the date this CI was first documented by your office. The amended date or reactivation date is not to be included in this box.

**Box 46:** The date signed by the first-line supervisor is the date of documentation, amended date, or reactivation date, depending on the type of CI documentation being generated.

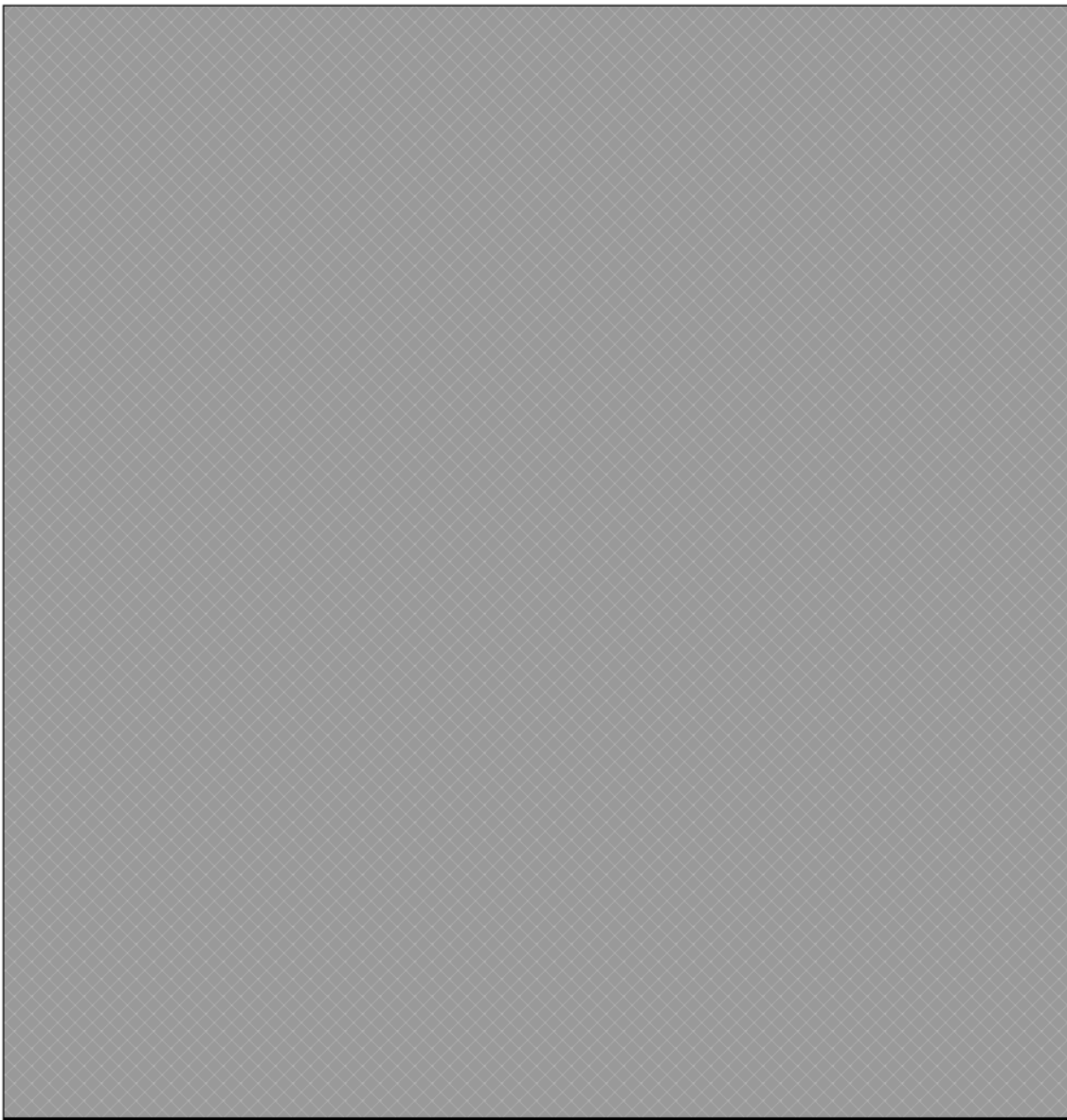
**Box 47:** Once the CI documentation is complete, it must be reviewed by the FCPA. The FCPA will initial this box to show that the review was completed.





DEPARTMENT OF HOMELAND SECURITY U.S. Immigration and Customs Enforcement				
<b>CONFIDENTIAL TRANSACTION RECEIPT</b>				
1. Control Number	2. ICE Office	3. Obligation No.	4. CUC Program Code	5. Date
6. Confidential Informant No. (If Applicable)	7. Case Number	8. Related FP&F Numbers		
<b>PAYMENT REQUEST</b>				
9. Type of Transaction	10. Funding Source (If other, indicate funding type in box 11)		11. If Other, Specify	
12. Enter Amount of Funds Requested (Type out)			13. Dollars \$	
16. Requesting Agent (Name/Title/Office)		17. Date	18. Requesting Agent's Signature	
19. Final Approving Official (Name/Title/Office)		20. Date	21. Approving Official's Signature	
<b>PAYMENT BY DEBIT CARD/CHECK</b>				
22. Debit Card Doc Number		23. Check Number		24. Check Amount \$
25. HQ/Local Approver			26. Date Approved	
27. Name/Title/Office of Agent Providing Funds/Check		Signature of Agent Providing Funds/Check		
28. Name/Title/Office of Agent Receiving Funds		Signature of Agent Receiving Funds		29. Date Funds Received
30. Name/Title/Office of Agent Making Payment		Signature of Agent Making Payment		31. Date Funds Paid
<b>TRANSFER OF FUNDS BY WIRE</b>				
32. Amount of Funds Received \$	TITLES AND SIGNATURES OF AGENTS RECEIVING FUNDS (Two Signatures Required)	33. Print Name/Title/Office		34. Signature
35. Date Funds Received		36. Print Name/Title/Office		37. Signature
<b>RETURN OF UNUSED FUNDS</b>				
38. Amount of Funds Returned (Type out)		\$	39. Method of Return	40. Date of Return
41. Name/Title/Office of Agent Returning Funds		Signature of Agent Returning Funds		
42. Name/Title/Office of Witnessing Agent		Signature of Witnessing Agent		
<b>RECEIPT OF FUNDS</b>				
43. Received from U.S. Immigration and Customs Enforcement (ICE) for information provided to ICE in furtherance of an ICE investigation. Funds awarded for information provided to ICE are considered to be taxable income to the recipient and are required to be reported to the Internal Revenue Service.				
44. Amount of Funds Received			\$	
45. Moiety Status <input type="checkbox"/> This payment is in lieu of Moiety <input type="checkbox"/> This payment is to be deducted from Moiety Initials of CI's Assumed Name: _____		46. Date Funds Received		
48. Signature of Witnessing Agent		49. Signature of Witnessing Agent		
50. Print Name/Title/Agency		51. Print Name/Title/Agency		

Part 2 – Mission Support, Financial and Logistics Management (FLMU)  
ICE Form 73-049 (3/16) Certified Undercover (CUC) Operation, if CUC operational funds are used. Dallas Finance Center (DFC) Page 2 of 4



RECEIPT OF FUNDS

43. Received from U.S. Immigration and Customs Enforcement (ICE) for information provided to ICE in furtherance of an ICE investigation. Funds awarded for information provided to ICE are considered to be taxable income to the recipient and are required to be reported to the Internal Revenue Service.

44. Amount of Funds Received \$

<p>45. Moiety Status</p> <p><input type="checkbox"/> This payment is in lieu of Moiety</p> <p><input type="checkbox"/> This payment is to be deducted from Moiety</p> <p>Initials of CI's Assumed Name: _____</p>	<p>46. Date Funds Received</p>	
---	--------------------------------	--

48. Signature of Witnessing Agent	49. Signature of Witnessing Agent
-----------------------------------	-----------------------------------

50. Print Name/Title/Agency	51. Print Name/Title/Agency
-----------------------------	-----------------------------



Field Confidential Informant Program Administrator's Signature

DEPARTMENT OF HOMELAND SECURITY U.S. Immigration and Customs Enforcement

IMMIGRATION BENEFITS RECEIPT

Form with fields 1-18: Control Number, Confidential Informant No., ICE Office, CUC Program Code, Case Number, Date, Type of Immigration Benefit, Recipient, Period of Authorization, Reason for the Benefit, Requesting Agent, Approving Official, etc.

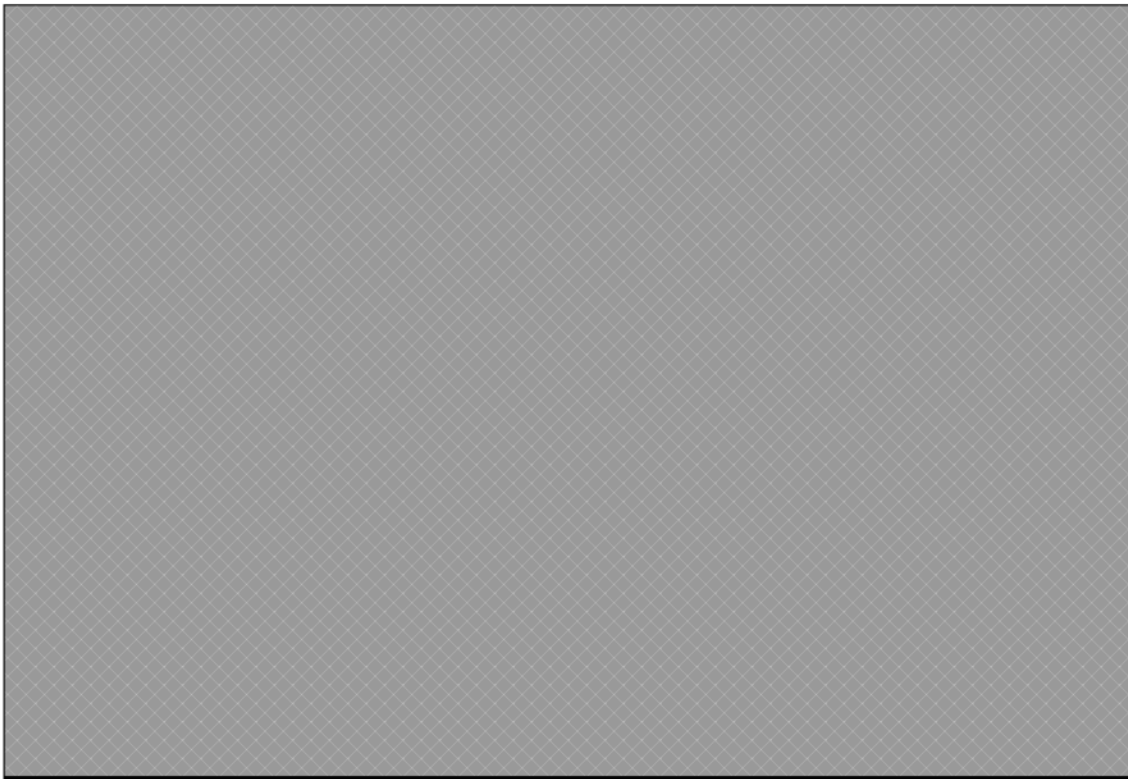
RECEIPT OF IMMIGRATION BENEFITS

Received from U.S. Immigration and Customs Enforcement (ICE) the following immigration benefit for cooperation in the investigation of violations of laws enforced by ICE. Benefits provided by ICE are subject to all applicable laws, regulations, and policy and may be revoked at any time in accordance with the terms of the program under which the benefit was provided.

Form with fields 19-23: Type of Immigration Benefit, Recipient, Assumed Name Signature of the CI, Date Benefit is Received, etc.

WITNESSING SIGNATURES

Form with fields 24-27: Print Name/Title/Agency, Signature of Witness, etc.



**RECEIPT OF IMMIGRATION BENEFITS**

Received from U.S. Immigration and Customs Enforcement (ICE) the following immigration benefit for cooperation in the investigation of violations of laws enforced by ICE. Benefits provided by ICE are subject to all applicable laws, regulations, and policy and may be revoked at any time in accordance with the terms of the program under which the benefit was provided.

19a. Type of Immigration Benefit (if other, indicate benefit type in next box)		19b. If other, indicate benefit type	
20. Immigration Benefit Recipient (If other, indicate relationship in the next box)		21. If other, indicate relationship, e.g., SA-123-HQ (Relationship Type)	
22. Assumed Name Signature of the CI			23. Date Benefit is Received

**WITNESSING SIGNATURES**

24. Print Name/Title/Agency	25. Signature of Witness
26. Print Name/Title/Agency	27. Signature of Witness



Item No.

INSTRUCTIONS

- Top box **The Field Confidential Informant Program Administrator's Signature** is a digital signature. The document is to be reviewed before submitting to the approving official. Signature ensures that the form is completed correctly, the CI file is up to date and complete, and justification documentation has been provided for this benefit request.
- 1 Control number will be current date (entered as YYYYMMDD), military time (hours and minutes), and Confidential Informant (CI) number (Do not put SA) (e.g., 123HQ). If a benefit will be received by a Cooperating Defendant (CD), input the abbreviation followed by the office code in the third section of the control number, e.g., CDHQ.
  - 2 Confidential Informant number.
  - 3 Select the ICE Office from the drop-down box.
  - 4 If the CI is involved in a case that is under a Certified Undercover operation then provide the program code for the operation.
  - 5 Enter the investigating office case number.
  - 6 Select today's date.
  - 7a Select the type of immigration benefit being provided.
  - 7b If type of benefit is not listed under Section 7, provide benefit type.
  - 8 Select the immigration benefit recipient, if not described in box 8 then indicate in box 9.
  - 9 Indicate the individual receiving the immigration benefit if not described in box 8.
  - 10 Enter the period of authorization for the immigration benefit provided, e.g., One year - January 1, 2016 through January 1, 2017
  - 11 Enter the assumed name of the CI receiving the benefit or their real name if Other. If the benefit is being provided to an immediate family member of a CI, the assumed name of the CI should be entered here.
  - 12 Provide justification for providing the benefit.
  - 13 Type name, title, and office of agent requesting the benefit.
  - 14 Signature of Requesting agent.
  - 16 Type name, title, and office of approving official.
  - 17 Signature of Approving Official.
  - 19a Auto populates from information provided in box 7a.
  - 19b Auto populates from information provided in box 7b.
  - 20 Auto populates from information provided in box 8.
  - 21 Auto populates from information provided in box 9.
  - 22 Signature of Recipient, if the recipient is a CI or a member of a CI's immediate family the CI will sign using his/her assumed name.
  - 23 Write the date the recipient received the benefit.
  - 24-27 Printed names, titles, agencies and signatures of witnesses.







WHERE TO SEND COPIES OF RECEIPT FOR IMMIGRATION BENEFITS

- PART 1 PLACE IN CI'S FILE AND SEND COPY TO HQ CI FILE CUSTODIAN  
 PART 2 PROVIDE RECEIPT TO CI



## Attachments

### Confidential Informant (CI) Attachments

Instructions to Confidential Informant	 CI Instructions.pdf
ICE Form 73-050 Immigration Benefits	 ICE Form 73-050.pdf
ICE Form 73-293 Benefit Transaction Receipt	 ICEForm-73-293-Con fidentialSourcePayme
ICE Form 73-015 Source Card	 ICE Form 73-015_Source Card.
Confidential Informant Documentation	 ICE Form 73-045.pdf
ICE Form 73-049 Confidential Transaction Receipt	 ICE Form 73-049.pdf

# *Counterterrorism Resources*



## **Combating Terrorism Center at West Point**

(b)(7)(E)



## **National Counterterrorism Center**

Intelligence Guide for First Responders:

(b)(7)(E)

Counterterrorism Guide:

(b)(7)(E)



## **Washington Institute for Near East Policy**

(b)(7)(E)

# START

NATIONAL CONSORTIUM FOR THE  
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

University of Maryland, START  
Center

(b)(7)(E)



Potomac Institute for Policy Studies, International  
Center for Terrorism Studies

(b)(7)(E)

**FDD's LONG WAR**  
JOURNAL 

Foundation for the Defense of  
Democracies, Long War Journal

(b)(7)(E)





# HSI Academy National Security HSI Special Agent Training Program



## **Terminal Performance Objective**

Given indicators of a potential national security threat, identify terrorism typologies, tactics and threats, as well as risk factors and indicators, in order to take appropriate investigative action in accordance with HSI policies and procedures.



## **Enabling Performance Objectives**

Define and describe terrorism and identify HSI's role in counterterrorism including the agency authorities which can be applied in counterterrorism investigations. Identify terrorism typologies, tactics, and applicable laws. Describe the fundamental elements of Islam. Demonstrate an understanding of Islamic culture, customs, and traditions.



## **Enabling Performance Objectives (cont'd)**

Describe Salafi-Jihadism and the ideological roots of modern Islamist terrorism. Recognize risk factors and indicators of radicalization and mobilization. Describe the U.S. national security architecture and a HSI SA's interaction with that architecture on national security counterterrorism matters. Demonstrate knowledge of HSI's NSID programmatic areas, NSID policies and procedures, as well as the characteristics of NSID investigations.

## Review of the Past

Having completed CITP and much of HSISAT, you have a basic working knowledge of criminal investigations and HSI authorities. In this lesson, you will be exposed to the nature of certain national security threats facing our nation and how HSI's unique authorities play a key role in confronting these threats. Additionally, you will be provided with HSI's policies, procedures, and practices relating to counterterrorism and national security.



## Main Ideas

The HSI National Security mission is vital in protecting the United States through enhancing national security investigations, preventing acts of terrorism by targeting the people, money and materials that support terrorist and criminal activities, and identifying and eliminating vulnerabilities in the nation's border, economic, transportation and infrastructure security.



# Agenda

HSI's role in counter-terrorism

Joint Terrorism Task Force

Use of Terrorist Identities Datamart Environment (TIDE)

Counterterrorism and Criminal Exploitation Unit

How to verify student status

Criminal charges related to terrorist crimes

NSID Human Rights Violators and War Crimes Unit

Demonstration scenario illustrating these elements

Practice activities with various scenarios

**HSI  
Academy**



# Define Terrorism

**“the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”**

**“Terrorism”**: a political term which was applied to the “Jacobin” revolutionaries in late 18th Century France and, in particular, those connected to the Revolutionary Tribunals during the “Reign of Terror.”<sup>1)</sup>  
Hence, terrorism: is inherently and fundamentally political in nature. “Terrorism” is about power and the achievement of political change – that power being the power of violence.<sup>2)</sup>  
The term “terrorism” was first popularized during the French Revolution.





# Domestic Terrorism

Title 18 U.S.C.  
§2331(5) – Involves  
acts dangerous to  
human life that  
violate federal or  
state law that are  
intended to:

- Intimidate or coerce a civilian population or portion thereof
- Influence the policy of a government by intimidation or coercion; or
- Affect the conduct of a government by mass destruction, assassination, or kidnapping



# Two General Criteria for “Domestic” Classification

Domestic terrorists operate in the US (i.e. their operations occur primarily within the territorial jurisdiction of the U.S.).

Domestic terrorists lack foreign inspiration; they are not inspired or enabled by Foreign Terrorist Organizations.



# Domestic Terrorism Examples

Right-wing Extremist Groups

Left-wing Terrorist Groups

(b)(7)(E)



# International Terrorism: 18 USC §2331(1)

Involves violent acts or acts dangerous to human life that violate federal or state law

Appears to be intended to: 1) Intimidate or coerce a civilian population  
2) Influence the policy of a government by intimidation or coercion; or  
3) Affect the conduct of a government by mass destruction, assassination, or kidnapping

Perpetrated by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations engaged in state-sponsored terrorism

International terrorism also includes homegrown violent extremists (HVEs) who are motivated by an ideology espoused by either by foreign actors or terrorist groups



**HSI Brings Unique  
Capabilities and  
Authorities to Bear on  
National Security  
Investigations**



# Border Search Authority

Can be used to encounter individuals, at the border, believed to be traveling in or otherwise supporting or involved in Terrorist activities

(b)(7)(E)



# Financial Investigations

Financial Crimes Enforcement Network  
(FinCEN) data

Egmont Requests – Financial intelligence  
sharing from foreign partners

Process Agreements – (b)(7)(E)

(b)(7)(E)



(b)(7)(E)

# Case Example

Following the 2015 Paris Attacks, HSI Special Agents

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)





# HSI and the Joint Terrorism Task Force

HSI is the single largest contributor of personnel to JTTF outside of the FBI.

(b)(7)(E)

Almost half of JTTF disruptions employ HSI authorities.

The HSI Headquarters element that has oversight over HSI participation on the JTTF is co-located with the FBI Headquarters Counterterrorism Division (CTD).



## Other HSI Investigative- Programmatic Areas with Potential Impacts on NS/CT Issues

- Counter-Proliferation
- Cyber Crimes Investigations including Computer Intrusion
- Identify and Benefit Fraud
- Human Smuggling
- Critical Infrastructure and Worksite Immigration Enforcement and Student-Exchange Visitors
- Human Rights Violators and War Crimes
- Commercial Fraud including enforcement of Intellectual Property Rights



# Other HSI Authorities/Investigative Capabilities That Can Impact NS/CT investigations

Mutual Legal Assistance Treaties

Undercover Operations

Administrative Immigration Enforcement Authorities

Administrative Process

Bank Secrecy Act Record Access

Money Laundering Statutes

Electronic Surveillance/T-III

**HSI  
Academy**



# Other HSI Authorities/Investigative Capabilities that can impact NS/CT investigations

HSI International Footprint via Attaché Offices and liaisons to DOD COCOMs

Ability to investigate international conspiracies

Bulk Cash Smuggling Investigative Authority



# Organizational Make-Up of Terrorist Groups

Terrorist groups  
have a  
centralized  
leadership  
hierarchy  
which:

(b)(7)(E)

These tasks are accomplished through a well-structured division of labor amongst the organizations' leadership and membership.

2021-ICLI-00031 Sup 2552



# Organizational Make-Up of Terrorist Groups

Terrorist groups have an ability to carry out sophisticated and well-coordinated attacks involving varied logistical support and detailed operational execution.

- Terrorist groups can involve simultaneous action by multiple members or cells of the group

Often, terrorist groups have more sophisticated financial networks which include the use of informal value transfer systems (IVTS), money remission services, and layered financial accounts allowing for wire transfers and the flow-through of funding from source to operatives.



# The Terrorist Attack Cycle

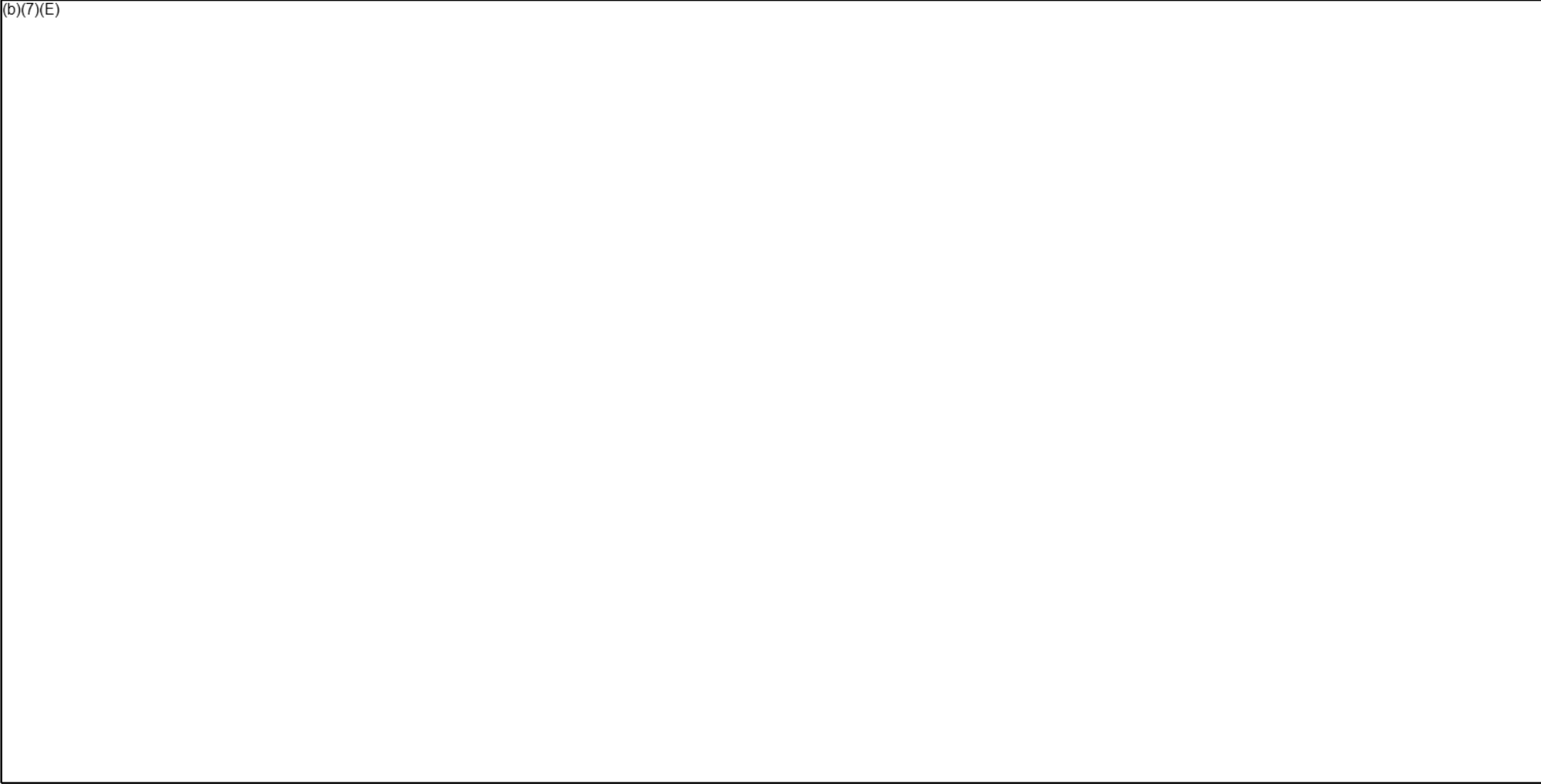
(b)(7)(E)

**HSI**  
**Academy**



# The Terrorist Attack Cycle

(b)(7)(E)

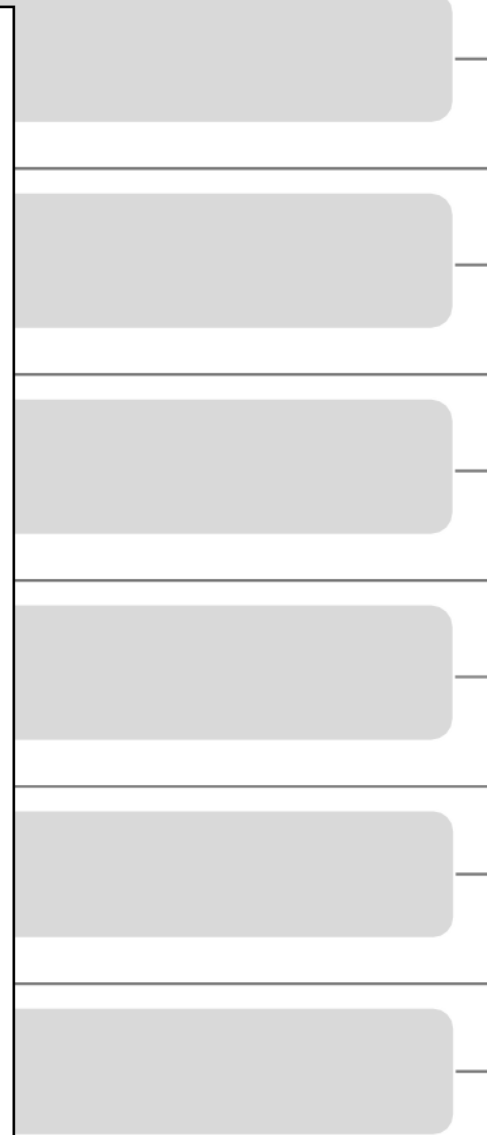
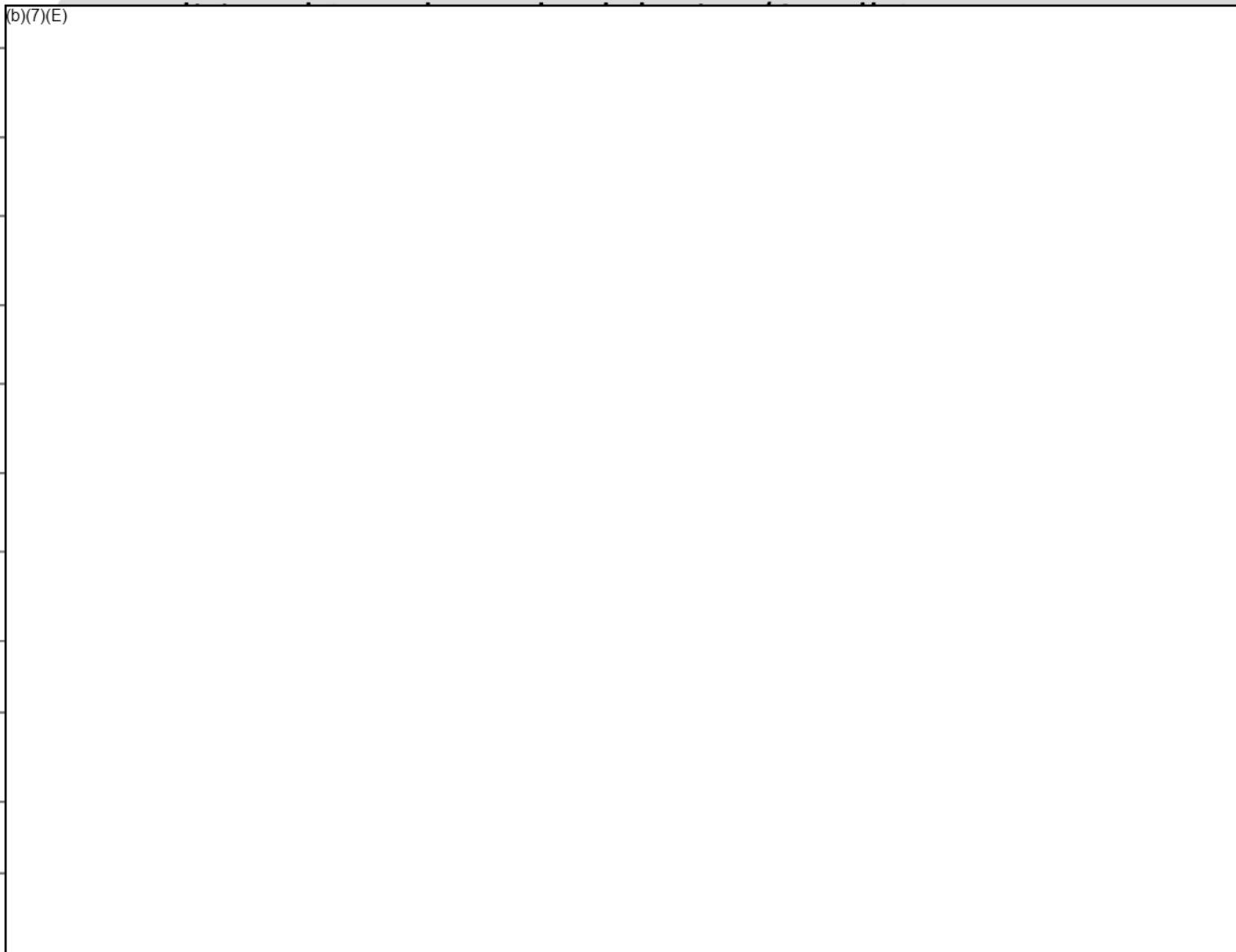




# Terrorist Training/Techniques/Practices (TTPs)

**HSI  
Academy**

(b)(7)(E)



# Terrorism Acts – Offenses

## 18 U.S.C. 2332: Murder of a U.S. National

- The killing of a U.S. National
- The attempted killing of a U.S. National
- Conspiring to kill a U.S. National
- Engaging in physical violence with the intent to cause serious bodily injury to a U.S. national or with the result that serious bodily injury is caused to a U.S. national

Written certification from the Attorney General or designee for criminal prosecutions that the offense was intended to coerce, intimidate, or retaliate against a government or a civilian population.



# Terrorism Acts – Offenses

## 18 U.S.C. 2332a: Use of Weapons of Mass Destruction

- It is unlawful to attempt, conspire, or threaten to use a weapon of mass destruction against U.S. persons or property used in interstate commerce.
- Weapon of Mass Destruction is defined broadly (*see Student Guide*).



# Terrorism Acts – Offenses

## 18 U.S.C. 2332b: Acts of Terrorism Transcending National Boundaries

- Prohibited Conduct:
  - Killing, maiming, kidnapping, or assault resulting in serious bodily injury, or assaults with a dangerous weapon of any person within the U.S., OR
  - Creating a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the U.S. or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the U.S., AND
  - In violation of any State or Federal Law, AND
  - Involves conduct which transcends national boundaries

• (b)(7)(E)

- Statute *also proscribes attempts, conspiracies, and threats* to commit the above prohibited conduct



# Terrorism Acts – Offenses

**18 U.S.C.  
2332d:  
Financial  
Transactions  
with Nation  
Designated as  
a State Sponsor  
of Terrorism**

- Covers any financial transactions with countries which have been designated by the U.S. State Department as State Sponsors of Terrorism
- Includes transactions with any official governmental agency or organization of that Terrorist State
- There are currently four (4) State Sponsors of Terrorism:
  - Iran (1984)
  - Syria (1979)
  - North Korea (2017)
  - Sudan (1993)
- Would cover transactions involving the central or official state banks of these countries



# Terrorism Acts – Offenses

## 18 U.S.C. 2332f: Bombings of public places, infrastructure, transportation, or Government facilities

- Act must be accompanied by an intent to:
  - Cause death or serious bodily injury, OR
  - Cause extensive destruction of such a place, facility, or system, where such destruction results in or is likely to result in major economic loss



# Terrorism Acts – Offenses

## 18 U.S.C. 2332g: Prohibited Activities Concerning Anti- Aircraft Missile Systems

- This statute prohibits the manufacture, sale, transfer, brokering the sale or transfer, and/or export of anti-aircraft missile systems
  - Unless such activity is licensed by the U.S. Government

(b)(7)(E)

- 



# Terrorism Acts – Offenses

## 18 U.S.C. 2332h: Prohibited Activities Concerning Radiation Dispersal Devices

- This statute prohibits the manufacture, sale, transfer, brokering the sale or transfer, and/or export of devices designed to disperse radiation
  - Unless such activity is licensed by the U.S. Government

(b)(7)(E)





# Terrorism Acts – Offenses

## 18 U.S.C. 2332i: Acts of Nuclear Terrorism

- This statute prohibits the knowing and unlawful possession of radioactive material or making or possession of such a device with the intent to:
  - Cause death or serious bodily injury, OR
  - Cause substantial damage to property or the environment
  - The statute also covers the intentional dispersal of radioactive material or contamination or exposure thereto.
- This statute covers attempts, conspiracies and threats to commit any of the delineated offenses involving radioactive material or related devices.



# Terrorism Facilitation – Offenses

**18 U.S.C.  
2339A:  
Material  
Support to  
Terrorists**

**Material support is defined as:**

- a) Property, both tangible and intangible
- b) Service
- c) Currency or monetary instruments or financial securities
- d) Financial services
- e) Lodging
- f) Training
- g) Expert advice or assistance
- h) Safe houses
- i) False documentation or identification
- j). Communications equipment or facilities
- k Weapons or explosives
- l) Lethal substances
- m) Personnel
- n) Transportation



# Terrorism Acts – Offenses

## 18 U.S.C. 2339A: Material Support to Terrorists (cont'd)

- Support must be “knowing and intending” for the commission of one of the predicate offenses:
  - Multiple specifically identified offenses per the statute
  - Federal Crimes of Terrorism listed in 2332b(g)(5)(B)
- The statute proscribes both providing “material support” and concealing “the nature, location, source, or ownership” of which support.
- The statute also proscribes attempts to provide Material Support and Conspiracies designed to provide Material Support to Terrorists in the commission of specifically delineated predicate offenses.



# Terrorism Acts – Offenses

## 18 U.S.C. 2339B: Material Support to Terrorists Organizations

- Material Support statutes are the most common prosecutorial tool, with 2339B being the most commonly used statute.
- The statute targets those who provide material support to designated Terrorist Organizations.
- Mens Rea (Knowledge) Requirement:
  - Subject must know that the foreign terrorist group to whom material support is provided is a:
    - Designated Terrorist Organization (Designated by the U.S. State Department), OR
    - That the terrorist group engages in or has in engaged in terrorism or terrorist activity



# Terrorism Acts – Offenses

## 18 U.S.C. 2339C: Prohibitions Against Financing Terrorism (Terrorist Financing)

- Proscribes the unlawful and willful provision or collection of funds with the intention or knowledge that they are to be used, in full or in part, to carry out a terrorist attack
- Predicate acts:
  - Offense prohibited under international law by a counterterrorism treaty, OR
  - Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.



# Terrorism Acts – Offenses

## 18 U.S.C. 2339D: Receipt of Terrorist Training

- Proscribes individuals from knowingly receiving “military-type training” from or on behalf of a foreign terrorist organization
  - Includes: Training in means or methods that can cause death or serious bodily injury, destroy or damage property, or disrupt services to critical infrastructure
  - Includes: Training on the use, storage, production, or assembly of any explosive, firearm or other weapon
  - Mens Rea (Knowledge) Requirement:
    - A subject, in order to be liable under this statute, as with 18 U.S.C. 2339B, must know that the foreign terrorist organization from which he is receiving military-type training is either a designated terrorist organization or engages in or has engaged in terrorism or terrorist activity.



# Terrorism Acts – Offenses

## 18 U.S.C. 2339: Harboring/ Concealing Terrorists

- Prohibits harboring or concealing any person whom the subject knows or has reasonable grounds to believe has committed, or is about to commit any of the following offenses:
  - 18 U.S.C. 32 – destruction of aircraft or aircraft facilities
  - 18 U.S.C. 175 – biological weapons
  - 18 U.S.C. 229 – chemical weapons
  - 18 U.S.C. 831 – related to nuclear materials
  - 18 U.S.C. 844(f) paragraphs (2) and (3) – arson and bombing of government property risking or causing injury or death



# Terrorism Acts – Offenses

## 18 U.S.C. 2339: Harboring/ Concealing Terrorists (cont'd)

- Prohibits harboring or concealing any person whom the subject knows or has reasonable grounds to believe has committed, or is about to commit any of the following offenses:
  - 18 U.S.C. 1366(a) – destruction of an energy facility
  - 18 U.S.C. 2280 – violence against maritime navigation
  - 18 U.S.C. 2332a – weapons of mass destruction
  - 18 U.S.C. 2332b – acts of terrorism transcending national boundaries
  - 42 U.S.C. 2284(a) – sabotage of nuclear facilities or fuel
  - 49 U.S.C. 46502 – aircraft piracy





**The Fundamental  
Elements of Islam**



# Why Learn About Islam?

Statistically, domestic terrorism is responsible for more violence in the United States than international terrorism. However, HSI does not have a significant role in domestic terrorism investigations.

June 2020

Conversely, HSI has a principal role in international terrorism investigations, and in the contemporary era; the international terrorism threat manifests from groups ideologically aligned with a very narrow and extreme expression of the Islamic faith.

2021-ICLI-00031 Sup 2573

HSI  
Academy



42

# The Religion of Islam: Six Major Beliefs (1 of 3)

## Belief in the Oneness of God

- God is the Creator of All Things
- God is All-Powerful and All-Knowing
- God has no Form
  - No Race, Gender, or Body
  - God has no offspring

## Belief in the Angels of God

- Muslims believe in unseen beings who worship God and do God's bidding
- Angel Gabriel is believed to have brought divine revelation to the Prophets (including Muhammad) and the Quran to Prophet Muhammad



# The Religion of Islam: Six Major Beliefs (2 of 3)

## Belief in the Books of God

- Muslims believe God revealed holy books/scriptures to a number of God's Messengers (i.e. Prophets)
- Though all believed to be divine and given to Prophets recognized in Islam – the Quran is supreme and is the only remaining revelation from "God" as first revealed to Muhammad

## Belief in the Prophets (Messengers) of God

- Muslim's believe guidance from God has been revealed to humankind through specially appointed messengers or prophets throughout history



# The Religion of Islam: Six Major Beliefs (3 of 3)

## Belief in the Day of Judgment

- On the Day of Judgment humans will be adjudged for their actions
- Those who followed God's guidance will be rewarded with paradise and those who have rejected God's guidance will be punished with hell

## Belief in the Divine Decree

- Everything in life is governed by Divine Decree
- Whatever happens in one's life is pre-ordained



# The Religion of Islam: Five Pillars of Islam

Declaration of Faith (called Shahada): “Allah is the one true God and Muhammad is his Messenger”

Prayer (called Salat): 5 times a day – dawn, noon, midafternoon, sunset, and night

Charity (called Zakat)

Fasting (Sawm)

Pilgrimage to Mecca (Hajj)



# Islamic Nations

Many people have a mistaken belief not only about the religion of Islam, the beliefs and practices of Muslims but also as to where most of the World's Muslim population is located.

- Many think “Arab” is synonymous with “Muslim.” While the majority population of Arab countries is Muslim, the majority of the world's Muslims do not originate from Arab countries.
- In fact, only about 1/5th of the World's Muslim population is located in the Arab world.



# Islamic Demographics: Most Populous Nations

Indonesia

Egypt

Pakistan

Iran

India

Turkey

Bangladesh

Algeria

Nigeria

Sudan

HSI  
Academy

June 2020

Islam is the 2nd largest religion worldwide, and fastest growing

2021-CL-005, slip 2579

48





# Islamic Demographics: Other Nations

Iraq: >38 Million

Philippines: >5 Million

Saudi Arabia: >31 Million

France: >4.5 Million

China: >24 Million

Thailand: >5 Million

Russia: >9 Million

USA: >approx. 3.5 Million



# History of Islam

## Caliphate and Caliph

- 570 C.E. Muhammad is born in Mecca.
- 610 C.E. Muhammad is visited by the Angel Gabriel in a cave near Mecca and makes the first revelations of the Quran to Muhammad.
- 622 C.E. Muhammad and his followers migrate to a nearby town now known as Medina (then called Yathrib) where the people accepted the teachings of Islam.
  - This emigration by Muhammad to Medina marks the beginning of the Islamic Calendar.
  - It is here that Muhammad establishes the first Islamic State (Caliphate) based on the laws revealed in the Quran and the divine inspiration he received from God.
- 630 C.E. Muhammad returns to Mecca. Eventually all of Mecca's citizens accept Islam.
- 633 C.E. Muhammad dies.
- Successors: Abu Bakr; Umar Ibn Al-Khattab; Uthman Ibn Affan; Ali ibn abu Talib
- 661 C.E. After the assassination of Ali, Muawiya ascends to the role of Caliph.



# Sunni vs. Shiite (Shia):

## Differences Explored

The split between Sunni and Shiite (Shia) Islam occurred over who would be the rightful successor to the Prophet Muhammad. Shia believe Ali ibn abu Talib, the being the closest thing to Muhammad's son and father to Muhammad's only grandsons, should be the rightful Successor.



# Sunni vs. Shiites

Between 80% and 90% of the World's Muslims are Sunni with between 10-20% identified as Shiites. (Much smaller sects exist which align with these two predominant sects but because of the sparseness are not statistically significant).

While both Sunnis and Shiites share the holy book of the Quran, Sunnis rely on records of teachings and sayings of Prophet Muhammad, known as the Sunnah (hence – Sunn-i), to guide their actions. Shiites tend to rely more on their Ayatollahs whom they believe to be a sign of God on earth.



**Islamic Culture,  
Customs and Traditions**



# Islamic Culture, Customs and Traditions

It should be noted that there is no “standardized” global Islamic culture, or even standard Islamic Arab culture

- Greetings
- Hospitality
- Body Language
- Naming Conventions
- Public Segregation



**Salafi-Jihadism and the  
ideological roots of  
modern Islamist  
terrorism**



# Hanbali School

**A sub-sect or school of Sunni Islam – the most conservative and strictest form of Sunni Islam**

- Adheres to a strict interpretation of the Koran and Sunnah, the writings of the Prophet Mohammad
- Famous disciple in the Islam Tradition is a 14th Century Muslim scholar named Ibn Taymiyyah
- Influenced Mohammad Ibn Abdul Wahhab – the 18th Century Islamic Scholar who created the doctrine of Wahhabism
- The Hanbali school also heavily influenced the pan-Islamist doctrine known as Salafism





# Jihad

The literal translation of “*Jihad*” (Arabic) is “struggle.”

Though often interpreted in the West to mean a “violent struggle,” *jihad* in Islam has multiple meanings

- *Jihad al-nafs*: (“Struggle of self”) is an internal struggle referring to a Muslims’ struggle with their own sinful nature and the never-ending search for righteousness
- *Jihad bil-qalam*: (“Struggle of the pen”) is an external struggle, whereby a Muslim engages in debate or persuasion for the good of *Allah*
- *Jihad bis-saif*: (“Struggle by the sword”) is an external armed struggle against an enemy



# Political Islam and Salafist-Jihadist Terrorism

**Islamism**: The belief that Islam should form the central, organizing structure around which all of society is organized

- Islamism grew in popularity as a reaction to European Imperialism and accelerated following WWII when many of the European powers were bringing their colonial periods to an end.

**Muslim Brotherhood**: arguable the most influential Islamist movement to emerge in the 20<sup>th</sup> Century

- A transnational Sunni Islamist movement seeking to establish a global caliphate under Shari'a law
- Founded in Egypt by Hassan al Banna in 1928
- Began as a pan-Islamic religious and social movement



# Sayyid Qutb and Salafism

## Sayyid Qutb :

- A leading ideologue of the Muslim Brotherhood during the 1950s and 1960s
- Writings disseminated across the Arabian Peninsula and the world
- Advocates for “Violent Jihad” and the killing of secular Muslims in order to implement Sharia
- Provided significant intellectual and theological underpinnings to modern Salafist-Jihadist terrorist groups, including al-Qa’ida and ISIS

## Salafism

- Building on the ideas of Sayyid Qutb and other intellectual elites in Islamist circles, Salafism has gained ground in the 20th and 21st centuries
- Salafism promotes the idea that Islam has been corrupted over the years by unorthodox and impermissible innovations
- Therefore, the only way to return to an authentic practice of Islam is to return to the ways of the Salaf, or “pious ancestors,” who were the contemporaries of the “rightly-guided” companions of the Prophet Muhammad



# Directed, Enabled, and Inspired Attacks by Salafi-Jihadist and Non-Salafi-Jihadist Organizations

(b)(7)(E)

**HSI  
Academy**



# Salafi-Jihadist Terrorist Groups

## Islamic State of Iraq and Syria (ISIS)

- Founded by Abu Bakr Al Baghdadi after the “Awakening” period in Iraq
- Further bolstered by Civil War in Syria when Sunni extremist groups entered Syria to fight the Syrian regime
- What later became ISIS was the largest insurgent group in Syria allowing it to declare itself the Islamic “State” of both Iraq and Syria
- Known for their use of social media and ability to inspire ISIS affiliates in areas beyond Iraq and Syria

(b)(7)(E)

June 2020

## Katibat al-Battar al-Ibi (KBL)

- Founded by Libyan Jihadists; KBL recruited and trained Libyan and Tunisian fighters who then went to fight in the Syrian civil war for KBL in alignment with ISIS
- Pledged allegiance to ISIS and Abu Bakr Al Baghdadi in 2014 when Al Baghdadi declared himself to be Caliph for a new Caliphate

(b)(7)(E)



# Salafi-Jihadist Terrorist Groups

## ISIS – Khorasan (ISIL-K)

- Formed in 2014 after six former senior members of the Tehrik-e-Taliban Pakistan pledged allegiance to IS Leader Abu Bakr al Baghdadi.
- The group receives funding directly from ISIS sources as well as overseas sympathizers via hawala networks.

(b)(7)(E)

## Al-Qaeda

- Al Qa'da (AQ) was formed in 1988, during the latter stages of the Soviet-Afghan war, by Osama Bin Laden. It is a Pan-Islamist, Sunni terrorist group formed with the goal of waging a global jihad and to fight back against the perceived imperialism of Western nations in the Muslim world. As such, the group adheres to the ideologies and doctrines found in Salafism, Qutbism, and Takfirism.
- AQ is a jihadist network that seeks to establish a caliphate, a global Muslim State, which operates under Sharia (Islamic) law. There are three cornerstones of AQ's doctrine.



# Al-Qaeda Affiliates

## Al Qa'da in the Arabian Peninsula (AQAP)

- AQAP, like its parent AQ, is a Sunni jihadist group which follows an ideological strain of Qutbist, Salafist, and Takfiri thought. The group was formed in 2009 from the merging of AQ affiliated groups in Saudi Arabia and Yemen.
- Many of AQAP's leaders and founders have strong ties to AQ and Osama bin Laden. Many traveled to Afghanistan in the late 1990's and early 2000s to train at AQ camps.
- The group has carried out violent jihadist attacks both domestically and internationally in service of Al Qa'ida's ideology.

June 2020

## Al-Qa'ida in the Islamic Maghreb (AQIM)

- AQIM, like AQ at large, is a Sunni jihadist group which follows an ideological strain of Qutbist, Salafist, an Takfiri thought. It is also known as *Jamaat Nusrat al-Islam wal Milimeen* (JNIM) which name began to be used following merger between AQIM and local, smaller salafist groups in the region. Despite this, the group still identifies as AQIM and is under the direction of AQ.

(b)(7)(E)



# Al-Qaeda Affiliates

## Al-Qa'ida in the Indian Subcontinent (AQIS)

- Founded in 2014 by AQ leader Ayman Al-Zawahiri.
- Like AQ proper, AQIS follows a Salafist ideology with a central tenet of waging “physical jihad” to impose sharia law and establish a caliphate in the Indian subcontinent. To that end, AQIS is active not just Afghanistan and Pakistan but in India, Burma, Bangladesh (AQIS branch referred to a Ansar al Islam), and Kashmir.

(b)(7)(E)

June 2020

## Al Shabaab

- Sunni extremist group founded in 1996-1997 in Somalia by Ibrahim Hai Jaama' Al Afghani; the group grew out of the rebel group which fought with the Somalia regime during the Somali Civil War of the early 1990s.
- The group's ideology adheres to many of the radical Islamic doctrines; chiefly, Wahabism, Salafism, Qutbism, Takfirism.

(b)(7)(E)





# Prominent Non-Salafist Islamist Terrorist Groups

## Hezbollah (translation: “The Party of God”)

- Shi’a Extremist Group created with the help of Iran in the early 1980s under the pretense of fighting foreign occupiers in Lebanon which refuses the right of the Jewish State of Israel to exist
- Active in Terrorist Attacks against Israelis, the Jewish State of Israel, as well as American and Jewish targets around the world
- Hezbollah resembles a proxy force for the Government of Iran (GOI) and receives funding, training, and weapons through the Islamic Revolutionary Guard Corps (IRGC)



# Prominent Non-Salafist Islamist Terrorist Groups

## Boko Haram

- Formed in 2002 in by a Salafist cleric named Mohammed Yusuf.
- Focused on opposing western education and establishing a caliphate in Nigeria.
- Conducted attacks on Nigerian military and security forces and engaged in wholesale kidnappings of children, often girls. Most famously, conducted a 2013 kidnapping of 200 school girls from a town in Nigeria which captured the world's attention and condemnation.
- Affiliated with the Islamic State of Iraq and Al Sham (ISIS). Prior to this affiliation, Boka Haram maintained ties to AQIM. Various Boko Haram members had previously trained and fought with AQIM in Mali



**Recognize risk factors  
and indicators of  
radicalization and  
mobilization**



# Indicators of Radicalization and Mobilization

## Homegrown Violent Extremists (HVEs)

Persons of any citizenship who have lived and/or operated primarily in the U.S. or its territories who advocate, engage in, or prepare to engage in ideologically-motivated terrorist activities (to include providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization



# HVE Classification (1 of 4)

Based on a historical analysis of HVE events by an Interagency Analytic Focus Group formed by the National Counterterrorism Center, the following observable behaviors have been identified as possible indicators of an individual's preparation to engage in violent extremist activity

(b)(7)(E)



# HVE Classification (2 of 4)

Group A Indicators –

(b)(7)(E)

(b)(7)(E)



# HVE Classification (3 of 4)

Group B indicators –

(b)(7)(E)

(b)(7)(E)

(b)(7)(E)

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 



# HVE Classification (4 of 4)

## Group C Indicators –

(b)(7)(E)

(b)(7)(E)

- (b)(7)(E)
- 
- 
- 
- 
- 
- 
- 
- 
- 





# Homework Assignment

This research and presentation development should be completed as homework. Work with your group to develop a 5-minute presentation covering the following items:

- Origins
- Ideology
- Training, tactics, and procedures
- A major attack/event



# Class Assignment Presentation

Your group should be prepared to give your 5-minute presentation of the assigned terrorist group. Each presentation covers the following items:

- Origins
- Ideology
- Training, tactics, and procedures
- A major attack/event



# National Security Architecture

Terrorism, as a national security threat, is beyond the scope of any single U.S. Government agency to effectively respond and mitigate the threat. As a result, counterterrorism is an enterprise effort, requiring cooperation and coordination across a host of U.S. Government agencies.

(b)(7)(E)



# Terrorist Identities Datamart Environment (TIDE)

HSI  
Academy

Central repository of known or suspected international terrorist identities

(b)(7)(E)



# TIDE Nominations and Sub-Categories

TIDE Nominations

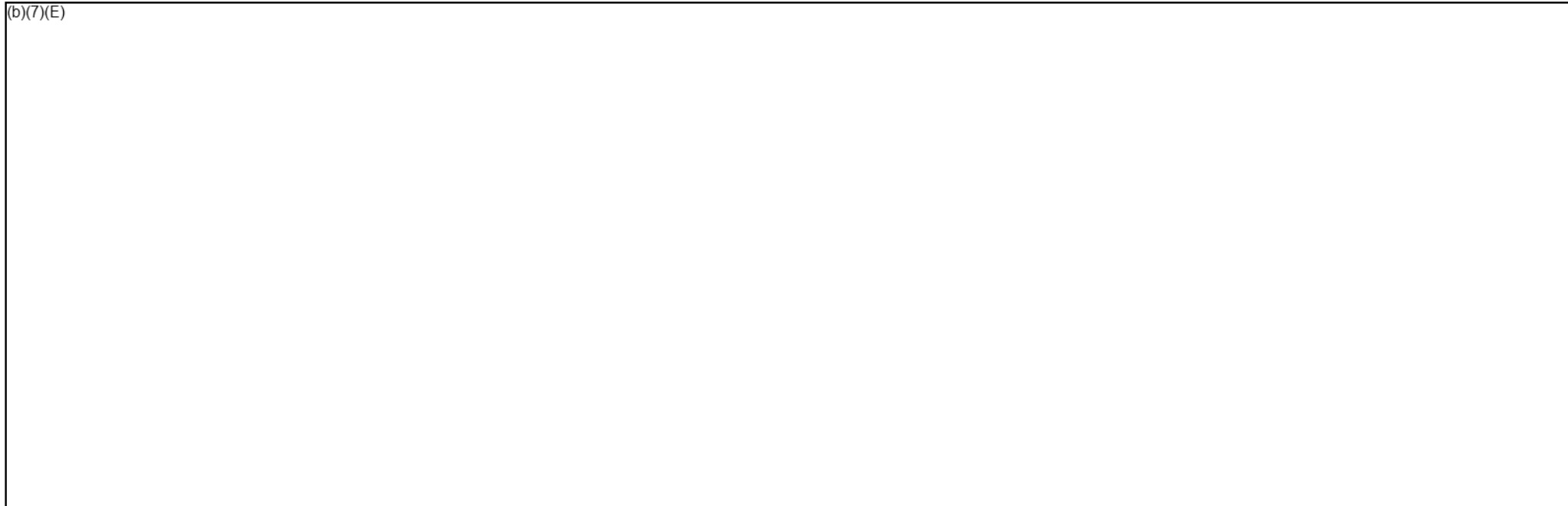
TIDE Sub-Categories

(b)(7)(E)



# TIDE Nominations and Sub-Categories

(b)(7)(E)



## Terrorist Screening Center (TSC)

- Created in 2003 as a result of the 9/11 attacks
- A Multi-Agency Center administered by the FBI
  - Other participants include members of federal law enforcement and other IC components.
  - Some TSC deputy positions held by DHS leadership.
- U.S. Government's Consolidated Counter-Terrorism Watch-Listing Component
- Maintains the Terrorist Screening Database (TSDB) – euphemistically known as “The Watchlist.”



# Terrorist Screening Database (TSDB)

**HSI  
Academy**

**Records**

**Subset of the TSDB**

(b)(7)(E)

--





# Handling Codes and B10 Records

## Prominent Handling Codes

(b)(7)(E)

(b)(7)(E)



## National Targeting Center (NTC)

(b)(7)(E)



# National Security and Counterterrorism Investigations

(b)(7)(E)

# HSI Academy



# National Security and Counterterrorism Investigations (cont'd)

**Immigration Status**

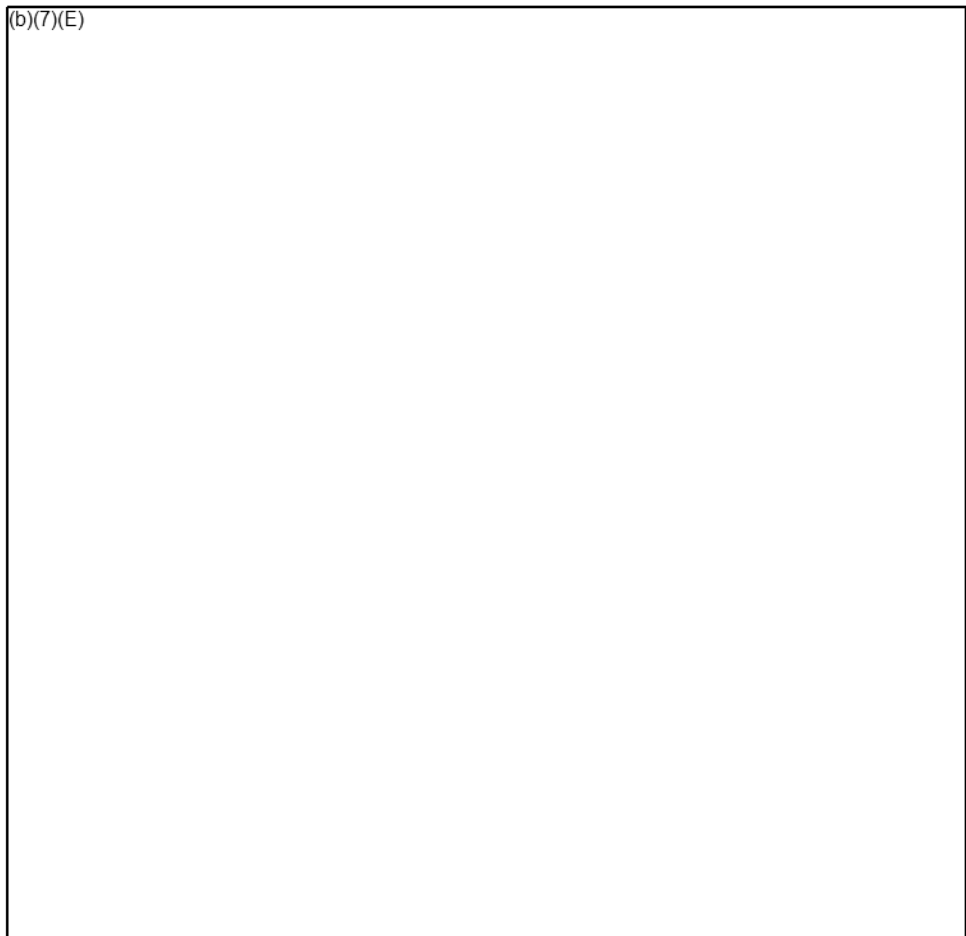
**Material Support Statutes**

(b)(7)(E)



# National Security and Counterterrorism Investigations (cont'd)

(b)(7)(E)



## Undercover Techniques

(b)(7)(E)



# Counterterrorism and Criminal Exploitation Unit

## Mission

- Prevent terrorists and related criminals from exploiting immigration system
- The mission is accomplished by:

(b)(7)(E)

## Oversight

- Oversees investigations related to nonimmigrant visa holders who violate their immigration status

■ (b)(7)(E)



## Counterterrorism and Criminal Exploitation Unit (cont'd)

### Targeting and Lead Generation

• (b)(7)(E)

### Lead Vetting and Verification

- Priority vetting
- HSI receives approximately 1.3-1.4 million potential leads each year considering possible violations of the nonimmigrant visa system.
- HSI routinely passes 800,000-900,000 of these leads to ERO.
- HSI engages in priority vetting and makes an assessment as to the viability of the lead. This results in less than 10,000 CTCEU leads being passed to HSI field offices annually.



## CTCEU Lead Assignment Process

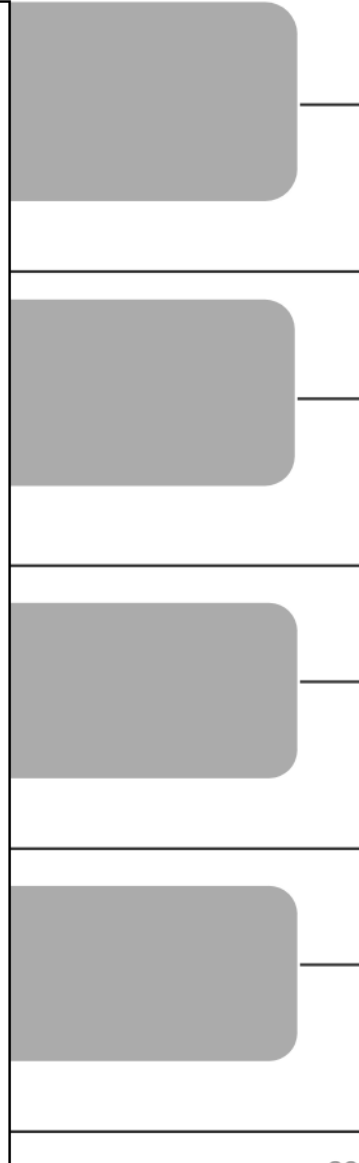
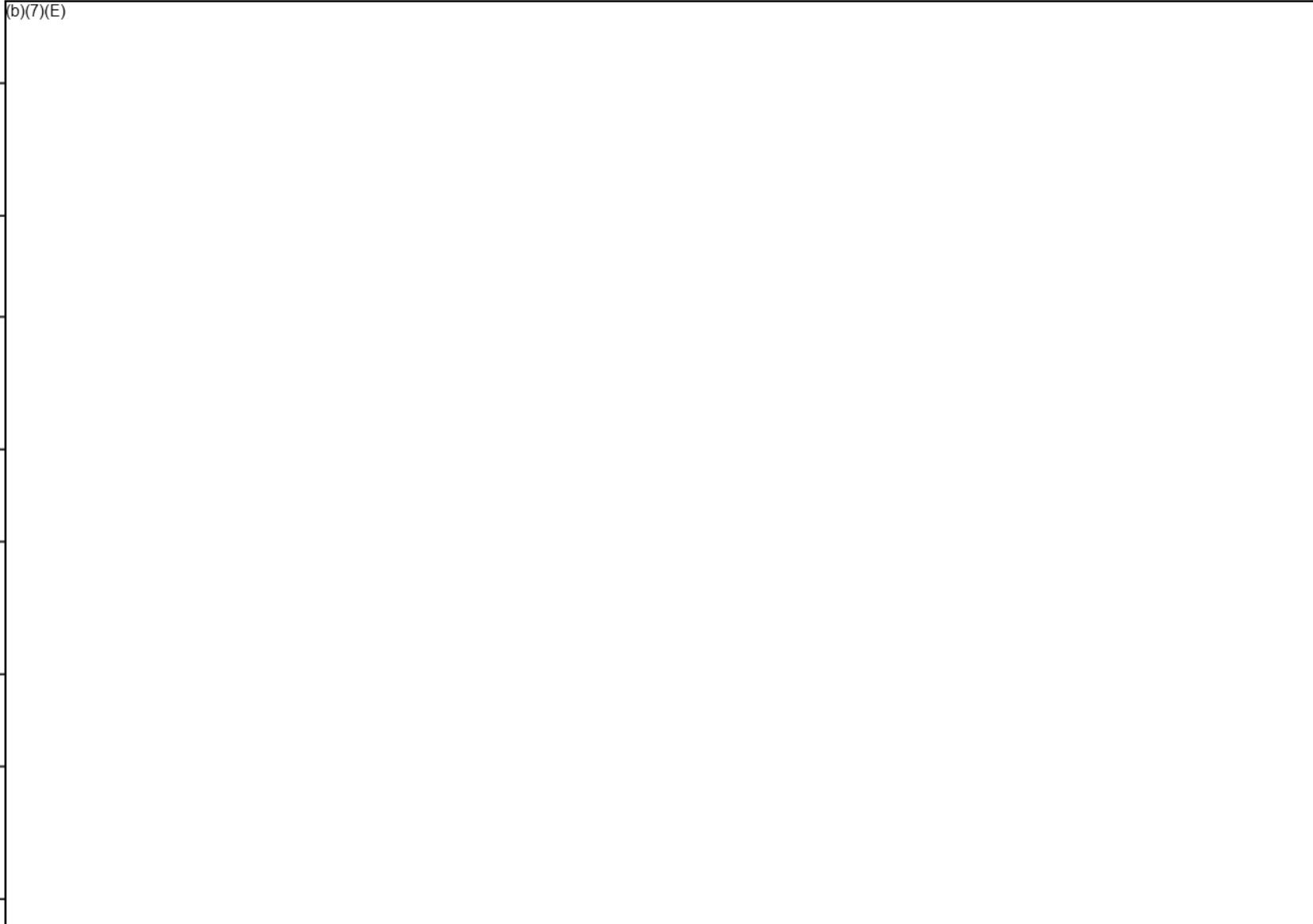
- Information uploaded into ICM ROI by HQ CTCEU
- ROI initiates collateral request for designated field office
- Field CTCEU coordinators review, assign collateral requests
- Case agent must post ROI to an opened investigation within 20 days of initiation of investigation
- If determined that subject is in another AOR, SA summarizes in closing ROI and reports it to CTCEU via ICM
- CTCEU initiates collateral request to field office for identified AOR





# When CTCEU Subject Located

(b)(7)(E)



**HSI  
Academy**



# If Unable to Locate CTCEU Subject

(b)(7)(E)



# Terrorist Nexus

- SAs working CTCEU investigations with a terrorist nexus: Contact their AOR's JTTF representative as soon as possible and before taking enforcement action.



## VISA Life-Cycle Program

- Goal is to allow HSI to continuously monitor, vet, and identify any derogatory information on foreign visitors which may arise during the validity for their respective non-immigrant visa.

(b)(7)(E)



# Student & Exchange Visitor Program (SEVP)



Collects, maintains, provides reliable information on foreign students and exchange visitors  
Program balances security with permitting legitimate foreign students and exchange visitors to participate in American academics



Maintains information on schools, programs certified by SEVP  
Includes Petition for Approval of School for Attendance by Nonimmigrant Student (Form I-17) and supporting documentation  
Requests for information or assistance from SEVP coordinated through CTCEU



## Student & Exchange Visitor Information System (SEVIS)

- Administered by SEVP
- Maintains accurate and current information on nonimmigrant students (F and M visa), exchange visitors (J visa), and their dependents (F-2, M-2, and J-2)
- Enables schools and program sponsors to transmit mandatory information and event notifications, via the Internet, to DHS and DOS throughout a student's or exchange visitor's stay in the U.S.
- Immigration Status vs. Visa Status



# DSOs and RSOs

- Designated School Official (DSO) – individual at academic institution inputting SEVIS data and issuing I-20s  
Responsible Officer (RO) – individual performing SEVIS duties for exchange visitor program  
DSOs/RSOs selected by own institution or not vetted by government



## SEVIS Exploitation Section (SES)

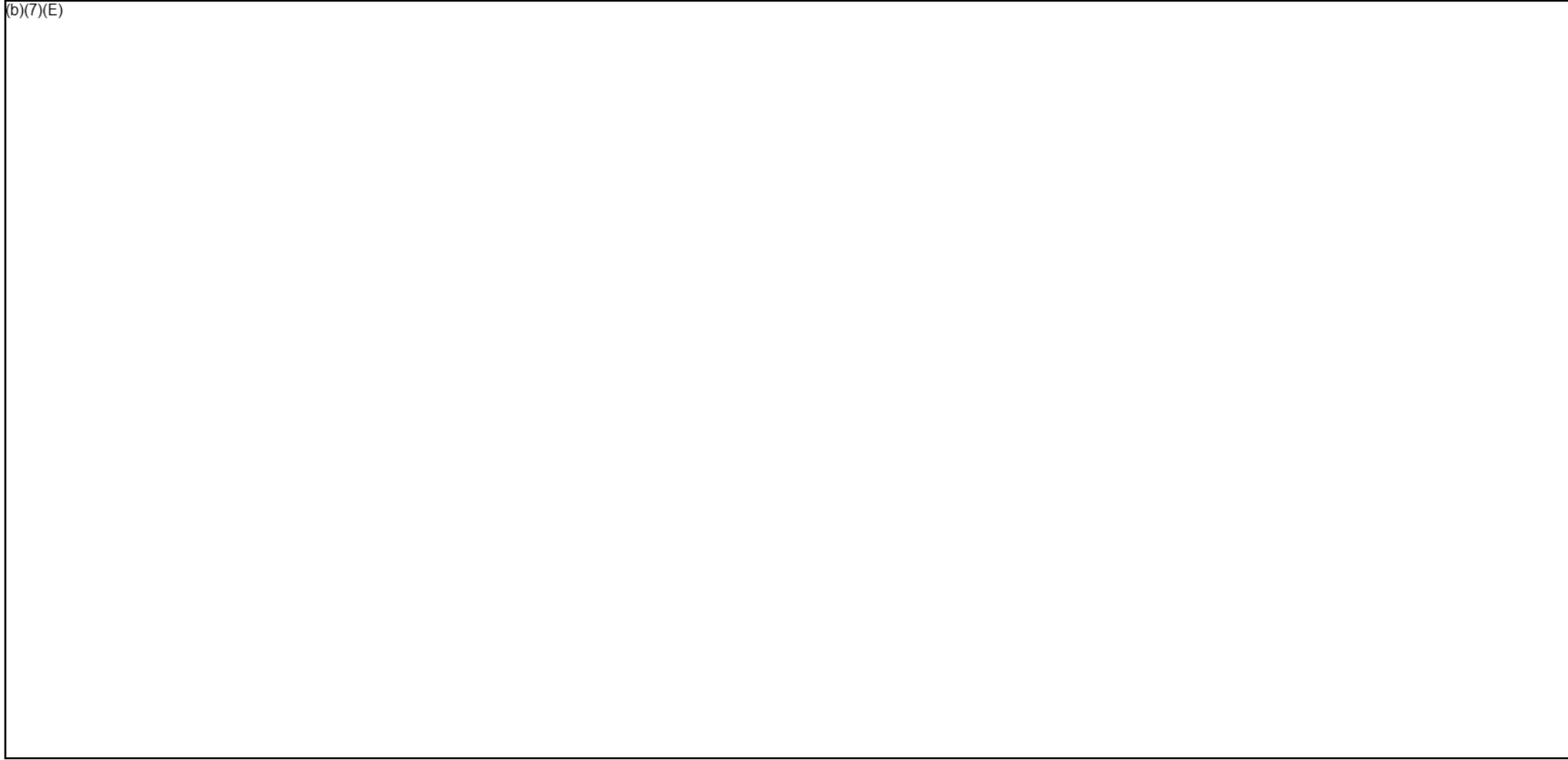
- Section within the CTCEU that combats criminal and administrative violations of the SEVP/SES carries out its mission by:  
Analyzing and referring school fraud criminal investigation leads to representatives in the field  
Implementing and managing an Agent/SEVIS School Outreach Program aimed at preventing the criminal exploitation of SEVP  
Development of SEVP field representative positions has assisted in maintaining more open and regular contact with participating institutions.  
SEVP representatives are assigned to certain districts around the U.S. and are assigned specific SEVP participating institutions in those districts with which to maintain contact and ensure compliance.





# Indicators of SEVP School Criminal Fraud

(b)(7)(E)



# Administrative Violations Relative to a Student Status Violator

(b)(7)(E)



# FERPA

- Federal law protecting privacy of student education records (20 U.S.C. § 1232g; 34 CFR Part 99) Applies to all schools that receive funds under an applicable program of the U.S. Department of Education Authority for Collecting Information 8 U.S.C. 1101 and 1184 Authorization to Release Information by School Student signs Form I-20 authorizing information release Recordkeeping DHS may request information concerning the student's immigration status for various reasons

## Family Educational Rights and Privacy Act



# Human Rights Violator and War Crimes Unit (HRVWCU)

- HSI is lead federal law enforcement agency charged with investigating Human Rights Violators and War Crimes  
Core Mission: “...to deny safe haven in the U.S. to human rights violators by utilizing all of ICE’s investigative techniques and legal authorities to identify, locate, investigate, prosecute and remove human rights violators, and war criminals from the U.S. to the U.S. of human rights violators and war criminals”



## HRVWCU Responsibilities

- Identifying suspected human rights violators
- Generating investigative leads which are then forwarded to the respective HSI field office(s)
- Providing intelligence, research, and coordinating intra-agency / international investigations
- Programmatic oversight of all HSI investigations relating to individual human rights violators, war criminals, and/or individuals implicated in acts of torture, genocide, or war crimes



# Human Rights Violator War Crimes Center (HRVWCC) and Components

- HRVWCU is a component of the overarching Human Rights Violator War Crimes Center.
- HSI is the lead executive agency for the HRVWCC.
- Human Rights Law Section (HRLS), a section within ICE's Office of the Principal Legal Advisor (OPLA), similarly situated under the HRVWCC umbrella.
- FBI's Genocide and War Crimes Unit (GWCU) also operates under the HRVWCC.
- HRT3 (Human Rights Violators Targeting and Tracking Team) seeks to identify foreign human rights abusers/war crimes suspects, and to "target" them in such a manner that they can be identified and properly vetted regarding their admissibility under the INA.



## Human Rights Violations and War Crimes (1 of 4)

- Substantive Charges are the initial focus of all HRVWC cases  
Substantive HRVWC charges include:
  - 8 U.S.C. 1091 – Genocide
  - 18 U.S.C. 2340a – Torture
  - 18 U.S.C. 2441 – War Crimes
  - 18 U.S.C. 2442 – Recruitment of and/or Use of Child Soldiers
  - 18 U.S.C. 181 – PeonageWhen possible, substantive charges can be used separately or in conjunction with the charges related to benefit fraud.



## Human Rights Violations and War Crimes (2 of 4)

- If substantive charges cannot be proved or where jurisdiction of these substantive offenses cannot or will not be exercised, HSI pursues criminal charges related to visa and benefit fraud.  
8 U.S.C. 1546 – Fraud and Misuse of Visa, Permits or other Documents  
18 U.S.C. 1425 – Unlawful Procurement of Citizenship or Naturalization  
18 U.S.C. 1001 – False Statements or Entries Generally  
18 U.S.C. 1621 – Perjury

(b)(7)(E)





# Human Rights Violations and War Crimes (3 of 4)

## Administrative Enforcement, under INA

Participation in Nazi  
Persecution

- § 212(a)(3)(E)(i)
- § 237(a)(4)(D)

Genocide

- § 212(a)(3)(E)(ii)
- § 237(a)(4)(D)

Torture

- § 212(a)(3)(E)(iii)(I)
- § 237(a)(4)(D)



# Human Rights Violations and War Crimes (4 of 4)

## Administrative Enforcement, under INA

### Extrajudicial Killing

- § 212(a)(3)(E)(iii)(II)
- § 237(a)(4)(D))

### Severe Violations of Religious Freedom

- § 212(a)(2)(G)
- § § 237(a)(4)(E)

### Recruitment or Use of Child Soldiers

- § 212 (a)(3)(G)
- §237(a)(4)(E)



# HRVWC Investigations – Lead Development

Leads for HRVWC cases can come from a variety of sources

(b)(7)(E)

(b)(7)(E)

**HSI  
Academy**



## Demonstration

(b)(7)(E)

- 
- 

See Demonstration Scenario in Student Guide



**Practice**

(b)(7)(E)

See Practice Scenario in Student Guide



## Summary

- Terrorism typologies, tactics, and applicable laws
- Fundamental elements of Islam and Islamic culture, customs, and traditions
- Salafi-Jihadism and the ideological roots of modern Islamist terrorism
- HSI's role in counterterrorism efforts requires collaboration with JTTF
- Overview of TIDE, CTCEU, SEVIS, and HRVWCU
- HSI's National Security Investigations Division (NSID) programmatic areas, NSID policies and procedures, as well as the characteristics of NSID investigations





**Protecting the  
Homeland with Honor,  
Service, and Integrity**

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



# **US Immigration and Customs Enforcement Homeland Security Investigations Training**

## **HSI Academy**



## **National Security 2103101**

### **Trainee Guide**

## **HSI Academy Courses**

~~WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). This contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, to anyone outside the HSI Academy, or to other personnel who do not have a valid "need-to-know" without prior approval of the HSI Academy Chief or his designee.~~





## National Security

### Motivation

(b)(7)(E)

### Objectives

#### Terminal Performance Objective (TPO)

**Conditions:** Given indicators of a potential national security threat,  
**Behavior:** identify terrorism typologies, tactics and threats, as well as risk factors and indicators, in order to take appropriate investigative action  
**Criterion:** in accordance with HSI policies and procedures.

#### Enabling Performance Objectives (EPOs)

- EPO 1:** Define and describe terrorism and identify HSI's role in Counterterrorism including the agency authorities which can be applied in Counterterrorism investigations.
- EPO 2:** Identify terrorism typologies, tactics, and applicable laws.
- EPO 3:** Describe the fundamental elements of Islam.
- EPO 4:** Demonstrate an understanding of Islamic culture, customs, and traditions
- EPO 5:** Describe Salafi-Jihadism and the ideological roots of modern Islamist terrorism.
- EPO 6:** Recognize risk factors and indicators of radicalization and mobilization.
- EPO 7:** Describe the United States' national security architecture and a HSI Special Agent's interaction with that architecture on national security counterterrorism matters.
- EPO 8:** Demonstrate knowledge of HSI's National Security Investigations Division (NSID) programmatic areas, NSID policies and procedures, as well as the characteristics of NSID investigations.

### Review of the Past

Having completed CITP and much of HSISAT, you have a basic working knowledge of criminal investigations and HSI authorities. In this lesson, you will be exposed to the nature of certain national security threats facing our nation and how HSI's unique authorities play a key role in confronting these threats. Additionally, you will be provided with HSI's policies, procedures, and practices relating to counterterrorism and national security.



## Advance Organizer of Main Ideas

The HSI National Security mission is vital in protecting the United States through enhancing national security investigations, preventing acts of terrorism by targeting the people, money and materials that support terrorist and criminal activities, and identifying and eliminating vulnerabilities in the nation's border, economic, transportation and infrastructure security.

## Agenda

During this lesson you:

- Discussed HSI's role in counterterrorism.
- Reviewed information on the Joint Terrorism Task Force (JTTF).
- Described the use of Terrorist Identities Datamart Environment (TIDE).
- Reviewed information on Counterterrorism and Criminal Exploitation Unit.
- Described how to verify student status.
- Discussed criminal charges related to terrorist crimes.
- Discussed the NSID Human Rights Violators and War Crimes (HRVWC) Unit.
- Completed practice activities with various scenarios.



## INSTRUCTION

### Explanation

**A. EPO 1: Define and describe terrorism and identify HSI’s role in Counterterrorism including the agency authorities which can be applied in Counterterrorism investigations.**

1. Definition: Terrorism is defined as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”
  - a. Origins of the word “Terrorism:” a political term which was applied to the “Jacobin” revolutionaries in late 18th Century France and, in particular, those connected to the Revolutionary Tribunals during the “Reign of Terror.”
    - 1) Hence, “terrorism” is inherently and fundamentally political in nature. “Terrorism” is about power and the achievement of political change – that power being the power of violence.
    - 2) The term “terrorism” was first popularized during the French Revolution.
2. Domestic terrorism
  - a. Domestic Terrorism – Title 18 U.S.C. §2331(5) – Involves acts dangerous to human life that violate federal or state law that are intended to:
    - 1) Intimidate or coerce a civilian population or portion thereof
    - 2) Influence the policy of a government by intimidation or coercion; or
    - 3) Affect the conduct of a government by mass destruction, assassination, or kidnapping
  - b. Two General Criteria to being Classified as “Domestic”
    - 1) Domestic terrorists operate in the U.S. (i.e. their operations occur primarily within the territorial jurisdiction of the U.S.)
    - 2) Domestic terrorists lack foreign inspiration.

They are not inspired or enabled by Foreign Terrorist Organizations.

### Examples

3) Right wing extremist groups

a)

b)

(b)(7)(E)



## Building

(1) Perpetrated by Timothy McVeigh and Terry Nichols, two individuals with survivalist, right-wing militia ties on April 19, 1995 (see below about date's importance) at the federal building which contained the offices of a variety of federal agencies (including ATF, DEA, and USSS). Among those killed were two U.S. Customs Special Agents, Paul Douglas and Claude Medearis.

(a) McVeigh, a prior U.S. Army Soldier and Persian Gulf War Veteran, was sentenced to death and executed in 2001. Nichols, another, U.S. Army veteran, where he met McVeigh, was sentenced to life in prison.

(2) Method of Attack: rental truck (Ryder) loaded with ammonium nitrate and fuel oil (ANFO)

(3) 168 People were killed, including 19 children, with more than 650 people injured. 300 buildings in the immediate were damaged.

(4) Motivations:

(a) Ruby Ridge Episode – 1992

Randy Weaver – a White Supremacist – an associate and his family engaged in a stand-off with Federal Agents in Idaho. Weaver had sold two sawed-off shotguns to ATF. After 11 Days, Weaver, Weaver's Associate, Kevin Harris, and Weaver's three daughters surrendered. During the siege, Weaver's 14 year-old- son was killed along with Weaver's wife. Deputy Marshall Michael Degan, USMS, was shot and killed during the siege.

(b) Branch Davidians in Waco – 1993

On February 28, 1993, ATF Agents raided the Branch Davidian Compound in Mt. Carmel, TX near Waco (Branch Davidians are a sect of the



Seventh Day Adventist Church). Four ATF Agents were killed and 15 wounded. Six Branch Davidians were killed and several more wounded. Following a seven-week standoff, on April 19, 1993, Federal Agents initiated a tear gas assault on the Mt. Carmel Compound. In a subsequent fire, which lit the compound ablaze, Koresh and 80 Branch Davidians, including 22 children died.

***April 19th is now a "holy" day for ultra right-wing militia and extremist group.***

4) Left wing terrorist groups)

- a) (b)(7)(E)
- b)

3. International Terrorism – Title 18 U.S.C. §2331(1)

- a. Involves violent acts or acts dangerous to human life that violate federal or state law
- b. Appears to be intended to:
  - 1) Intimidate or coerce a civilian population
  - 2) Influence the policy of a government by intimidation or coercion; or
  - 3) Affect the conduct of a government by mass destruction, assassination, or kidnapping
- c. Perpetrated by individuals and/or groups inspired by or associated with designated foreign terrorist organizations or nations engaged in state-sponsored terrorism
- d. International terrorism also includes homegrown violent extremists (HVEs) who are motivated by an ideology espoused by either by foreign actors or terrorist groups.
  - 1) Consequently, it is possible for an international terrorism incident to occur and be solely perpetrated by a U.S. born person where the incident was entirely planned, funded, and undertaken wholly within the United States without any foreign assistance or action.
  - 2) It is the motivation and ideology behind the terrorist attack that determines whether an incident or act is considered one of domestic terrorism or international terrorism.



4. HSI brings unique capabilities and authorities to bear on national security threats.

**Class Group Exercise**

(b)(7)(E)

a. Databases

1)

2)

3)

4)

5)

b. Authorities

1) HSI is the primary federal investigative agency for crimes involving people, money, and goods crossing borders.

2) Border Searches:

a)

b)

c)

d)



(b)(7)(E)

e)

3) Financial Investigations

- a) Financial Crimes Enforcement Network (FinCEN) data
- b) Egmont Requests – Financial intelligence sharing from foreign partners

c) Process Agreements – (i.e., (b)(7)(E))

(b)(7)(E)

(1) (b)(7)(E)

(2)

(3)

(4)

(5)

4) HSI and the Joint Terrorism Task Forces

- a) HSI is the single largest contributor of personnel to JTTF



- outside of the FBI.
- b) In FY18, HSI was a contributor in 78% of the 167 terrorist disruptions affected by JTTF nationwide.
  - c) Almost half of JTTF disruptions employ HSI authorities.
  - d) The HSI Headquarters element that has oversight over HSI participation on the JTTF is co-located with the FBI Headquarters Counterterrorism Division (CTD).
- 5) Other HSI Investigative-Programmatic Areas with potential impacts on NS/CT issues – a few include:
- a) Counter-Proliferation
  - b) Cyber Crimes Investigations including Computer Intrusion
  - c) Identify and Benefit Fraud
  - d) Human Smuggling
  - e) Critical Infrastructure and Worksite
  - f) Immigration Enforcement and Student-Exchange Visitors
  - g) Human Rights Violators and War Crimes
  - h) Commercial Fraud including enforcement of Intellectual Property Rights
- 6) Other HSI Authorities/Investigative Capabilities that can impact NS/CT investigations
- a) Customs Mutual Assistance Agreements
  - b) Mutual Legal Assistance Treaties
  - c) Undercover Operations
  - d) Administrative Immigration Enforcement Authorities
  - e) Administrative Process
  - f) Bank Secrecy Act Record Access
  - g) Enforce Money-Laundering Statutes
  - h) Electronic Surveillance and Title III Capabilities
  - i) Operation of Confidential Informants, both Foreign and Domestic
  - j) HSI International Footprint via Attaché Offices and liaisons to DOD COCOMs
  - k) Ability to investigate international conspiracies
  - l) Bulk Cash Smuggling Investigative Authority

**Notes:**





**B. EPO 2: Identify terrorism typologies, tactics, and applicable laws.**

1. Organizational make-up of terrorist groups

a. Terrorist groups have a centralized leadership hierarchy which:

- 1) (b)(7)(E)
  - 2)
  - 3)
  - 4)
  - 5)
- (b)(7)(E)

- b. Terrorist groups also engage in activities which seek to inspire others to commit sanctioned terrorist attacks and provide information on various means for doing so.
- c. Terrorist groups have an ability to carry out sophisticated and well-coordinated attacks involving varied logistical support and detailed operational execution.

Terrorist groups can involve simultaneous action by multiple members or cells of the group.

- d. Often, terrorist groups have more sophisticated financial networks which include the use of informal value transfer systems (IVTS), money remission services, and layered financial accounts allowing for wire transfers and the flow-through of funding from source to operatives.
- e. Terrorist groups can range from hundreds to thousands of avowed members.

2. Terrorist Attack Cycle

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

Page 2653

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2654

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2655

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

4. Terrorism acts – offenses
  - a. 18 U.S.C. 2332: Murder of a US National
    - 1) Proscribes
      - a) The killing of a U.S. National
      - b) The attempted killing of a U.S. National
      - c) Conspiring to kill a U.S. National
      - d) Engaging in physical violence with the intent to cause serious bodily injury to a U.S. national or with the result that serious bodily injury is caused to a U.S. national
    - 2) Written certification from the Attorney General or his designee for criminal prosecutions that the offense was intended to coerce, intimidate, or retaliate against a government or a civilian population
  - b. 18 U.S.C. 2332a: Use of Weapons of Mass Destruction
    - 1) It is unlawful to attempt, conspire, or *threaten* to use a weapon of mass destruction against U.S. persons or property used in interstate commerce.
    - 2) Weapon of Mass Destruction is defined broadly and includes:
      - a) Any explosive, incendiary, or poison gas including the following:
        - (1) Bomb
        - (2) Grenade
        - (3) Rocket having an explosive or incendiary charge of more than 4 ounces
        - (4) Missile having an explosive or incendiary charge of more than one-quarter ounce
        - (5) Mine
        - (6) Or any device similar to devices listed above



- b) Any weapon that is designed, or intended, to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors
  - c) Any weapon involving a disease organism; and
  - d) Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life
- c. 18 U.S.C. 2332b: Acts of Terrorism Transcending National Boundaries
- 1) Prohibited conduct
    - a) Killing, maiming, kidnapping, or assault resulting in serious bodily injury, or assaults with a dangerous weapon of any person within the U.S., OR
    - b) Creating a substantial risk of serious bodily injury to any other person by destroying or damaging any structure, conveyance, or other real or personal property within the U.S. or by attempting or conspiring to destroy or damage any structure, conveyance, or other real or personal property within the U.S., AND
    - c) In violation of any State or Federal Law, AND
    - d) Involves conduct which transcends national boundaries
  - 2) Charge is intended to target violent international terrorist activity that occurs within the U.S. where at least a part of that activity also occurs outside the U.S.
    - a) Includes conduct which targets persons or property within the U.S.
    - b) Conduct can be in violation of State or Federal Law
  - 3) Provides for a broad jurisdictional basis authorizing the U.S. Government the ability to arrest and prosecute offenders
  - 4) Statute *also proscribes attempts, conspiracies, and threats* to commit the above prohibited conduct
  - 5) 18 U.S.C. §2332b(g)(5) – defines the Federal crime of terrorism as:
    - a) An offense that is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct, AND
    - b) Violates any of the statutes listed in 18 U.S.C. §2332b(g)(5)(B)
- (b)(7)(E)
- d. 18 U.S.C. 2332d: Financial Transactions with Nation designated as a State Sponsor of Terrorism



- 1) Covers any financial transactions with countries which have been designated by the U.S. State Department as State Sponsors of Terrorism
  - 2) Includes transactions with any official governmental agency or organization of that Terrorist State
  - 3) There are currently four (4) State Sponsors of Terrorism:
    - a) Iran (1984)
    - b) Syria (1979)
    - c) North Korea (2017)
    - d) Sudan (1993)
  - 4) Would cover transactions involving the central or official state banks of these countries
- e. 18 U.S.C. 2332f: Bombings of public places, infrastructure, transportation, or Government facilities
- 1) Act must be accompanied by an intent to:
    - a) Cause death or serious bodily injury, OR
    - b) Cause extensive destruction of such a place, facility, or system, where such destruction results in or is likely to result in major economic loss
- f. 18 U.S.C. 2332g: Prohibited Activities Concerning Anti- Aircraft Missile Systems
- 1) This statute prohibits the manufacture, sale, transfer, brokering the sale or transfer, and/or export of anti-aircraft missile systems
    - a) Unless such activity is licensed by the U.S. Government
  - 2) 

(b)(7)(E)
- g. 18 U.S.C. 2332h: Prohibited Activities Concerning Radiation Dispersal Devices
- 1) This statute prohibits the manufacture, sale, transfer, brokering the sale or transfer, and/or export of devices designed to disperse radiation
    - a) Unless such activity is licensed by the U.S. Government
  - 2) 

(b)(7)(E)



h. 18 U.S.C. 2332i: Acts of Nuclear Terrorism

- 1) This statute prohibits the knowing and unlawful possession of radioactive material or making or possession of such a device with the intent to:
  - a) Cause death or serious bodily injury, OR
  - b) Cause substantial damage to property or the environment
- 2) The statute also covers the intentional dispersal of radioactive material or contamination or exposure thereto.
- 3) This statute covers attempts, conspiracies and threats to commit any of the delineated offenses involving radioactive material or related devices.
  - a) "Threats" Include:
    - (1) Threats which "may reasonably be believed"
    - (2) Threats used to demand possession of or access to radioactive material, a device, or a nuclear facility

5. Terrorism Facilitation -- Offenses

a. 18 U.S.C. 2339A: Material Support to Terrorists

- 1) Material support is defined as:
  - a) Property, both tangible and intangible
  - b) Service
  - c) Currency or monetary instruments or financial securities
  - d) Financial services
  - e) Lodging
  - f) Training
  - g) Expert advice or assistance
  - h) Safe houses
  - i) False documentation or identification
  - j) Communications equipment or facilities
  - k) Weapons or explosives
  - l) Lethal substances
  - m) Personnel

One or more individuals who may be or include oneself

- n) Transportation
- 2) Support must be "knowing and intending" for the commission of one of the predicate offenses:
  - a) Multiple specifically identified offenses per the statute





- b) Federal Crimes of Terrorism listed in 2332b(g)(5)(B)
  - 3) The statute proscribes both providing “material support” and concealing “the nature, location, source, or ownership” of which support.
  - 4) The statute also proscribes attempts to provide Material Support and Conspiracies designed to provide Material Support to Terrorists in the commission of specifically delineated predicate offenses.
  
- b. 18 U.S.C. 2339B: Material Support to Terrorist Organizations
  - 1) Material Support statutes are the most common prosecutorial tool, with 2339B being the most commonly used statute.
  - 2) The statute targets those who provide material support to designated Terrorist Organizations.
  - 3) Mens Rea (Knowledge) Requirement:
    - a) Subject must know that the foreign terrorist group to whom material support is provided is a:
      - (1) Designated Terrorist Organization (Designated by the U.S. State Department), OR
      - (2) That the terrorist group engages in or has in engaged in terrorism or terrorist activity
  
- c. 18 U.S.C. 2339C: Prohibitions Against Financing Terrorism (Terrorist Financing)
  - 1) Proscribes the unlawful and willful provision or collection of funds with the intention or knowledge that they are to be used, in full or in part, to carry out a terrorist attack
  - 2) Predicate acts:
    - a) Offense prohibited under international law by a counterterrorism treaty, OR
    - b) Any act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.
  
- d. 18 U.S.C. 2339D: Receipt of Terrorist Training
  - 1) Proscribes individuals from knowingly receiving “military-type training” from or on behalf of a foreign terrorist organization



- a) "Military-type training" includes:
    - (1) Training in means or methods that can cause death or serious bodily injury, destroy or damage property, or disrupt services to critical infrastructure
      - (a) Critical Infrastructure is defined as systems and assets vital to:
        - i. National defense
        - ii. National security
        - iii. Economic security
        - iv. Public health or safety
      - (b) "Critical Infrastructure" can include either regional or national infrastructure and can be publicly or privately owned.
    - (2) Training on the use, storage, production, or assembly of any explosive, firearm or other weapon
  - b) Mens Rea (Knowledge) Requirement
    - (1) A subject, in order to be liable under this statute, as with 18 U.S.C. 2339B, must know that the foreign terrorist organization from which he is receiving military-type training is either a designated terrorist organization or engages in or has engaged in terrorism or terrorist activity.
- e. 18 U.S.C. 2339: Harboring/Concealing Terrorists
- 1) Prohibits harboring or concealing any person whom the subject knows or has reasonable grounds to believe has committed, or is about to commit any of the following offenses:
    - a) 18 U.S.C. §32 – destruction of aircraft or aircraft facilities
    - b) 18 U.S.C. 175 – biological weapons
    - c) 18 U.S.C. 229 – chemical weapons
    - d) 18 U.S.C. 831 – related to nuclear materials
    - e) 18 U.S.C. 844(f) paragraphs (2) and (3) – arson and bombing of government property risking or causing injury or death
    - f) 18 U.S.C. 13B66(a) – destruction of an energy facility
    - g) 18 U.S.C. 2280 – violence against maritime navigation
    - h) 18 U.S.C. 2332a – weapons of mass destruction
    - i) 18 U.S.C. 2332b – acts of terrorism transcending national boundaries
    - j) 42 U.S.C. 2284(a) – sabotage of nuclear facilities or fuel



k) 49 U.S.C. 46502 – aircraft piracy

**Notes:**

**C. EPO 3: Describe the fundamental elements of Islam.**

1. Why learn about Islam?

(b)(7)(E)

2. The Religion of Islam (*Islam* in English translates as “submission”)

a. Customs and Practices

1) Six Major Beliefs

a) Belief in the Oneness of God

(1) God is the Creator of All Things

(2) God is All-Powerful and All-Knowing



- (3) God has no Form
  - (a) No Race, Gender, or Body
  - (b) God has no offspring
- b) Belief in the Angels of God
  - (1) Muslims believe in unseen beings who worship God and do God's bidding
  - (2) Angel Gabriel is believed to have brought divine revelation to the Prophets (including Muhammad) and the Quran to Prophet Muhammad
- c) Belief in the Books of God
  - (1) Muslims believe God revealed holy books / scriptures to a number of God's Messengers (i.e. Prophets)
    - (a) Quran to Muhammad
    - (b) Torah to Moses
    - (c) Gospel to Jesus
    - (d) Psalms to David
    - (e) Scrolls to Abraham
  - (2) Though all believed to be divine and given to Prophets recognized in Islam – the Quran is supreme and is the only remaining revelation from "God" as first revealed to Muhammad.
- d) Belief in the Prophets (Messengers) of God
  - (1) Muslim's believe guidance from God has been revealed to humankind through specially appointed messengers or prophets throughout history.
    - (a) 25 Prophets mentioned in the Quran include: Jesus, Moses, Abraham, and even the first man – Adam.
  - (2) Muhammad, to Muslims, is the LAST IN THE LINE OF THESE PROPHETS.
  - (3) Quran was revealed to Muhammad so that ALL humankind could receive the message of Islam.
- e) Belief in the Day of Judgment
  - (1) On the Day of Judgment humans will be adjudged for their actions



- (2) Those who followed God's guidance will be rewarded with paradise and those who have rejected God's guidance will be punished with hell.
- f) Belief in the Divine Decree
  - (1) Everything in life is governed by Divine Decree
  - (2) Whatever happens in one's life is pre-ordained
    - (a) To Muslims – they do not believe "Free-Will" to be affected because humans do not have prior knowledge of God's decree; hence, humans retain a freedom of choice.
    - (b) Good or bad events should still be met with the same thankfulness and patience.
- b. 5 Pillars of Islam
  - 1) Declaration of Faith (called Shahada): "Allah is the one true God and Muhammad is his Messenger."
    - a) Required for entry into Islam
    - b) Statement repeated by Muslims during their prayers
  - 2) Prayer (called Salat):
    - a) Prayer 5 times a day: dawn, noon, midafternoon, sunset, and night
    - b) Muslims go through ritual washing prior to prayer.
    - c) Face in direction of Mecca while praying
      - (1) Friday is the Muslim Holy Day.
      - (2) Friday noon prayer is the most special prayer and should be done at Mosque if at all possible.
  - 3) Charity (called Zakat)
    - a) Obligatory charity based on 2.5% of person's income and wealth
    - b) In addition, Muslims are encouraged to give voluntarily to charity throughout the year.
  - 4) Fasting (Sawm)
    - a) Fasting from dawn to dusk during the month of Ramadan
      - (1) Ramadan: The month in which the revelation of the Quran to Muhammad began



Quran revealed to Muhammad by Gabriel (the angel).

- b) Nightly gathering to “break-fast”
- c) Fasting includes refraining from food, liquids (including water), sexual activity, smoking, etc.
- d) Eid-Al-Fitr
  - (1) Festival of the Fast-Breaking
  - (2) Occurs on the first day of the month after Ramadan
  - (3) Involves celebrations, prayers, feasts, gift-giving

5) Pilgrimage to Mecca (Hajj)

- a) Travel to the holy city of Mecca in Saudi Arabia is required of every Muslim if financially and physically able.
  - (1) Mecca is home to the first house of worship of God (Allah) – The Kaaba

The Kaaba is believed to have been built by the Prophet Abraham and his son Ishmael.

- (2) Mecca is Muhammad’s Birthplace and where he lived when the first revelations of the Quran are said to have come to him and where he learns he is God’s (Allah’s) prophet.
- (3) 630 C.E.: Muhammad returned to Mecca from Medina (after being ostracized for his preaching Islam) and eventually all citizens of Mecca accept Islam.

The Kaaba is transformed: All Idols and Images are removed, and it is rededicated to the worship of God (Allah) alone.

- b) Eid al Adha
  - (1) Festival of the Sacrifice
  - (2) Second Major Holiday in Islam
  - (3) 10th Day of Month at the conclusion of the Pilgrimage
  - (4) Involves the Sacrifice of an Animal (Lamb or Goat)

Meat is distributed to relatives, friends, and the needy.

c. Islamic Nations



Only about 20% of the World's Muslims live in Arab Countries (Turkey and Iran are not Arab nations). More than 1 Billion Muslims Live in Asia.

1) General Discussion

- a) Many people have a mistaken belief not only about the religion of Islam, the beliefs and practices of Muslims but also as to where most of the World's Muslim population is located.
- b) Many think "Arab" is synonymous with "Muslim." While the majority population of Arab countries is Muslim, the majority of the world's Muslims do not originate from Arab countries.

- (1) In fact, only about 1/5th of the World's Muslim population is located in the Arab world.
- (2) "Arab" refers to the peoples descended from the Bedouin nomadic tribes that inhabited the Pre-Islamic Arabian Peninsula and Levant area.

Bedouin's were polytheistic and placed heavy emphasis on kin-related groups clustered as a clan under tribes

2) Islam: Demographics

- a) Islam is the 2nd largest religion in the world and is the fastest growing religion.
- b) Most populous Muslim nations (Top Ten)

- (1) Indonesia

Home to 12.7% of the world's Muslims

- (2) Pakistan

Depending on the Source India and Pakistan flip between second and third.

- (3) India
- (4) Bangladesh
- (5) Nigeria
- (6) Egypt
- (7) Iran
- (8) Turkey
- (9) Algeria
- (10) Sudan



c) Other Nations (of note) with high large numbers of Muslims:

- (1) Iraq – 11th (Over 38 Million)
- (2) Saudi Arabia – 14th (Over 31 Million)
- (3) China – 18th (over 24 Million)
- (4) Russia – 31st (Over 9 Million)
- (5) Philippines – 40th (Over 5 Million)
- (6) France – 45th (Over 4.5 Million)
- (7) Thailand – 50th (Nearly 4 Million)

United States has a population of approximately 3.5 Million Muslims (though some estimates are appreciably higher). Muslims make up approximately 1.1% of the total US population.

3. History of Islam

a. Caliphate and Caliph

- 1) 570 C.E. Muhammad is born in Mecca.
- 2) 610 C.E. Muhammad is visited by the Angel Gabriel in a cave near Mecca and makes the first revelations of the Quran to Muhammad; Muhammad is informed that he is God's Prophet. Muhammad begins preaching the teachings of Islam in Mecca but is met with hostility and persecution.
- 3) 622 C.E. Muhammad and his followers migrate to a nearby town now known as Medina (then called Yathrib) where the people accepted the teachings of Islam.
  - a) This emigration by Muhammad to Medina marks the beginning of the Islamic Calendar.
  - b) It is here that Muhammad establishes the first Islamic State (Caliphate) based on the laws revealed in the Quran and the divine inspiration he received from God. Muhammad successfully recruits other tribes and nations to Islam.
- 4) 630 C.E. Muhammad returns to Mecca. Eventually all of Mecca's citizens accept Islam. The Kaaba re-dedicated solely to the worship of God.
- 5) 633 C.E. Muhammad dies. Father-in-Law (and close associate), Abu Bakr, elected by Muslim Community as "Caliph" meaning Successor (First of the "Four Rightly Guided" Caliphs); member of Quraish Tribe.
- 6) 634 C.E. Abu Bakr dies; Umar Ibn Al-Khattab (Umar) is also of the Quraish Tribe (2nd of 4 "Rightly Guided" Caliphs); Umar was also the father of one of Muhammad's wives.
- 7) 644 C.E. Umar is assassinated; Uthman Ibn Affan appointed "Caliph" (3rd of 4 "Rightly-Guided" Caliphs).





- a) Uthman showed favoritism to the Umayyad clan to which his own family belonged.
  - b) Umayyads had initially opposed and fought Muhammad when he declared himself to be the Apostle of God.
  - c) This favoritism sowed discontent within the Muslim world, especially with Muhammad's son-in-law – Ali ibn abu Talib (Ali was also Muhammad's cousin and adopted son).
- 8) 638-655 C.E. Islam spreads into Al Sham Region (North of Arabian Peninsula), parts of Persia (modern day Iran), Egypt and across North Africa.
- 9) 656 C.E. Uthman assassinated in Medina; Ali ibn abu Talib selected as the 4th Caliph (Last of the 4 "Rightly-Guided" Caliphs); Tension between Ali and the Umayyad Governor of Syria, Muawiya (appointed by Caliph Uthman), erupts into civil war among Muslims.
- 10) 661 C.E. Ali assassinated and Muawiya, the Umayyad Governor of Syria, ascends to the role of Caliph.
- a) This initiates the major split in Islam between Shia, who regard Ali as Prophet Muhammad's true heir, and Sunni.

The idea for the 4 "Rightly-Guided" Caliphs comes from the belief that all four were the true adherents to the Sunnah – the teachings and sayings of Muhammad (also known as the Prophet's tradition). This idea of "rightly-guided," however, is a Sunni based belief. Shiites believe only Ali ibn abu Talib was fit to succeed Muhammad as Caliph.

b. Sunni and Shia: Differences Explored

- 1) The split between Sunni and Shiite (Shia) Islam occurred over who would be the rightful successor to the Prophet Muhammad. Shia believe Ali ibn abu Talib, being the closest thing to Muhammad's son and father to Muhammad's only grandsons, should be the rightful Successor.

The term "Shiite" is a contraction of the phrase Shiat Ali which means "Followers of Ali." Sunnis, on the other hand, do not recognize Ali as Muhammad's rightful Successor.

- 2) Between 80% and 90% of the World's Muslims are Sunni with between 10-20% identified as Shiites. (Much smaller sects exist which align with these two predominant sects but because of the sparseness are not statistically significant).

Most Shiite Muslims live in three countries: Iran, Iraq, and



Bahrain, with some in India and Pakistan as well.

- 3) While both Sunnis and Shiites share the holy book of the Quran, Sunnis rely on records of teachings and sayings of Prophet Muhammad, known as the Sunnah (hence – Sunn-i), to guide their actions. Shiites tend to rely more on their Ayatollahs whom they believe to be a sign of God on earth.
- 4) Both Groups follow the ritualistic 5 Pillars of Islam.
- 5) Shiites actually celebrate the anniversary of the death of Husayn (Hussein) ibn Ali, the son of Ali and grandson of Prophet Muhammad. This always occurs on the 10th day of the holy month of Muharram which is the first month in the Islamic lunar calendar. (This illustrates how Shiites revere the actual bloodline succession Muhammad as the true leaders of Islam).
  - a) Husayn was massacred with many relatives in Karbala (now in modern day Iraq) in 680 C.E.
  - b) Shiites observe “Ashoura” which is a collective atonement through lamentation and self-flagellation. This practice of “Ashoura” is unique to Shiites.
  - c) The Martyrdom of Husayn is a central tenet of Shiite Islam who believe Ali should have succeeded the Prophet Muhammad.
  - d) Sunnis do not celebrate the day or view it as important.
- 6) Though many Sunnis and Shiites co-habit peacefully, a 2012 study reported that 40% of Sunni Muslims from the Middle East and North Africa do not accept Shiites as fellow Muslims.

**Notes:**



**D. EPO 4: Demonstrate an understanding of Islamic culture, customs, and traditions.**

1. It should be noted that there is no “standardized” global Islamic culture, or even standard Islamic Arab culture, for that matter. However, there are common elements amongst the multitude of Islamic cultures globally. Keep in mind, these Islamic cultural norms may be “muted” when observed amongst the population of Muslims long resident in the United States or amongst Westerners who have adopted the faith.

a. Greetings

- 1) Handshakes – are frequently exchanged at the beginning and end of any meeting. However, they frequently are not as firm as those customary among Europeans or Americans. Men should not shake hands with a Muslim woman unless she offers her hand.
- 2) Touching – Particularly among Arabs – it is much more common for individuals of the same sex to touch each other as a show of friendship. It is not uncommon to see two men holding hands as they walk down the street. Conversely, physical contact between members of the opposite sex in public is considered nearly obscene.
- 3) Small talk – in Arab cultures, it is common for small talk and ritual greetings to take up what seems to be an inordinate amount of time to Westerners.
  - a) Asking about each other’s health and well-being is customary. However, do not directly ask a Muslim man about his wife or another female family member.
  - b) Do not make gestures or suggestions that you are hurried, such as looking at your watch. Time is less rigidly scheduled in many Islamic countries and they may be insulted by your actions.

b. Hospitality

- 1) Muslims often believe that some hospitality must be offered to individuals within their home.
- 2) The level of hospitality can reveal the level of comfort and rapport with the visiting individuals.
- 3) Beware of commenting too frequently about an item belonging to an individual who ascribes to the Muslim faith. Often the individual may, by matter of culture, feel obliged to gift the item.
- 4) Throughout Islamic cultures in Asia and the Middle East, the right hand is used to eat, touch, and present gifts. The left hand is generally regarded as unclean.
- 5) It is common to stand when someone enters the room.



- 6) It is common to take one's shoes off before entering a dwelling. Hosts occasionally leave oversized slippers at the entrance for you to wear inside the home.

Do not show the soles of your feet, as they are the lowest and dirtiest part of the body.

- 7) Touch and pass food with your right hand only.
- 8) Muslims are very particular about showing respect to elders.

c. Body Language

- 1) Social distance – Asians and Arabs, in particular, do not require as much personal space as Westerners.
- 2) Eye contact – Maintaining eye contact will likely make Muslim women uncomfortable. Young people, as well, have been taught it is disrespectful or challenging to stare into the eyes of authority figures. This aversion to eye contact should not be interpreted as a sign of deception.

d. Naming conventions among Arab Muslims

- 1) Arab Muslims have multiple names other than just a first and surname.
  - a) These Names Imply a Genealogical Relationship.
    - (1) Names include the father's and grandfather's name and the sequence shows the specific genealogical relationship.
    - (2) Father's name proceeds the grandfather name.

(b)(7)(E)

- (3) Traditionally, in Arab cultures, women keep their Father's name.

(b)(7)(E)

b) Use of *kunyah*

- (1) *Kunyah* is the Arabic term referring to the nicknames commonly adopted in the culture.
- (2) Examples:



- (a) “*Abu*” – Father or owner of
- (b) “**Umm**” – Mother of

- (3) Second part of the *kunyah* is the name of the oldest child or male child or a trait associated with the person.

- (a) 

(b)(7)(E)

- (b) location, and even profession. It is not uncommon for Muslims to use their *kunyah* in identifying themselves and each other.
- (c) It is important to remember, however, that a Muslim’s *kunyah* is not their true, legal name but is only a “nickname.”

c) Importance of family

- (1) The family forms the basic building block of Muslim society.
- (2) Several generations often live together, occupying the same dwelling, providing mutual support and security for each other.
- (3) Marrying and establishing a family is very strongly encouraged.
- (4) Families maintain tribal and clan connections and loyalties are strong, hence the expression, “I am my brothers against my cousins; I and my cousins against the stranger.”
- (5) Muslims often know and speak proudly of their genealogy.

d) Role of women – Historically, in Islam, women have not been treated as men’s equals.

- (1) Traditional examples
  - (a) Men have sole discretion as to the naming of children (he can let his wife be involved but he retains final say).
  - (b) Men decide if and when the women are covered in public – when the women shall wear the hijab.



Women are viewed often as a source of temptation and conflict.

- (c) Forced Marriages
- (d) Prevented from praying, fasting, or touching the Quran during menstruation and for a period after childbirth (during these times women are considered impure).

- (2) Notably, this viewpoint espousing the subjugation of women to their fathers and husbands has been retained by Wahabists and Salafists.

An unrelated male speaking to a female alone is not permitted absent permission from a male relation of that female. (b)(7)(E)

(b)(7)(E)

e) Public segregation

- (1) Many Muslim nations require and provide separate areas for women and men.
  - (a) Notably, the areas into which the women are allowed are considered “family” areas in which women, along with minor children of both sexes, and their male relatives (i.e. husbands, brothers, fathers) are allowed.
  - (b) Single males or unrelated males not accompanied by family are not allowed in these areas.
  - (c) These are separated from “male only” areas where, just as the name implies, only men can enter and occupy.

Traditionally, Mosques are regarded as male only spaces.

- (d) Muslim women do follow beliefs and Pillars of Islam.

Women can make the “hajj” and even interact with men during that pilgrimage and at religious shrines (non-Mosques).



- (e) Muslim homes often are designed with areas in mind for receiving visitors and other areas where guests will never venture. If the house is small, meetings will be timed so visitors do not interact with family members with whom they have no business.

**Notes:**

**E. EPO 5: Describe Salafi-Jihadism and the ideological roots of modern Islamist terrorism.**

1. Hanbali School
  - a. A sub-sect or school of Sunni Islam – the most conservative and strictest form of Sunni Islam
  - b. Adheres to a strict interpretation of the Koran and Sunnah, the writings of the Prophet Mohammad
  - c. Famous disciple in the Islam Tradition is a 14th Century Muslim scholar named Ibn Taymiyyah.
    - 1) Taymiyyah not only argued that Muslims should emulate the ways of the Prophet and his companions but that Islam in his time was being perverted by so called modern interpretations and the worship of saints he deemed to be false.
    - 2) He has also been venerated by some Muslims in the 19th and 20th Century for his arguments in favor of “jihad” and is stance that there is only the true Islamic world, one that strictly adheres to



the Prophet's tradition, and all else, regardless of pretension, is non-Islamic.

- d. Influenced Mohammad Ibn Abdul Wahhab – the 18th Century Islamic Scholar who created the doctrine of Wahhabism
  - 1) Wahhabism pushed for the strict adherence to the “pious predecessors” espoused by Hanbalists and Ibn Taymiyyah.
  - 2) Wahhabism also sought to add a “Sixth Pillar” to Islam – that of “Jihad.”
  - 3) Wahhabism came to prominence with the rise of the House of Saud in Saudi Arabia where it is the ultra-conservative Islamic ideology of this doctrine is the prevailing political system.
  - 4) Wahhabism was focused mainly on Muslim societies on the Arabian Peninsula.
- e. The Hanbali school also heavily influenced the pan-Islamist doctrine known as Salafism (See Below).

## 2. *Jihad*

- a. The literal translation of “*Jihad*” (Arabic) is “struggle.” Though often interpreted in the West to mean a “violent struggle,” “*jihad*” in Islam has multiple meanings:
  - 1) *Jihad al-nafs*: (“Struggle of self”) is an internal struggle referring to a Muslims’ struggle with their own sinful nature and the never-ending search for righteousness.
  - 2) *Jihad bil-qalam*: (“Struggle of the pen”) is an external struggle, whereby a Muslim engages in debate or persuasion for the good of *Allah*.
  - 3) *Jihad bis-saif*: (“Struggle by the sword”) is an external armed struggle against an enemy.
    - a) *Jihad bis-saif* is commonly understood to be permissible as a matter of self-defense, not as a justification to seek out and destroy non-believers (*kufar*). However, terrorist groups have sought to justify their violence by characterizing their campaigns as defensive.

## 3. Political Islam and the roots of Salafist-Jihadist Terrorism

- a. Islamism – the belief that Islam should form the central, organizing structure around which all of society is organized
- b. Islamism grew in popularity as a reaction to European Imperialism and accelerated following WWII when many of the European powers were bringing their colonial periods to an end.
- c. Muslim Brotherhood – arguable the most influential Islamist movement to emerge in the 20<sup>th</sup> century





- 1) A transnational Sunni Islamist movement seeking to establish a global caliphate under Shari'a law
- 2) Founded in Egypt by Hassan al Banna in 1928
- 3) Began as a pan-Islamic religious and social movement building popular support through political activism, social welfare initiatives, and proselytizing
- 4) Also had an armed wing dedicated to the eradication of British rule in Egypt and the Jewish presence in Palestine
- 5) Rejects "Western-Style" Nationalism – distinguished by the focus on Nation-States and instead espouses a "Pan-Islamic Nationalism" in which the Caliphate would not be defined by physical/geographic borders but by the range of peoples of the Islamic faith – regardless of racial or blood differences
- 6) One "*Umma*" – Global community of Muslims
- 7) Stands against a rise in secularism and the influence of Western culture in Muslim societies
- 8) Introduction of Islamic Sharia as the basis for controlling the affairs of state and society
- 9) Works to achieve unification among the Islamic countries and states, mainly among the Arab states, and liberating them from foreign imperialism
- 10) (b)(7)(E)

4. Sayyid Qutb

- a. A leading ideologue of the Muslim Brotherhood during the 1950s and 1960s
- b. Writings disseminated across the Arabian Peninsula and the world
- c. Advocates for "Violent Jihad" and the killing of secular Muslims in order to implement Sharia
- d. Popularized "*Takfir*" – doctrine by which Muslims serving a secular ruler (i.e. a non-Sharia Government and State leaders) are deemed apostates and, thereby, legitimate targets for execution
- e. Provided significant intellectual and theological underpinnings to modern Salafist-Jihadist terrorist groups, including al-Qa'ida and ISIS.

5. Salafism

- a. Building on the ideas of Sayyid Qutb and other intellectual elites in Islamist circles, Salafism has gained ground in the 20<sup>th</sup> and 21<sup>st</sup> centuries.
- b. Salafism promotes the idea that Islam has been corrupted over the years by unorthodox and impermissible innovations.
- c. Therefore, the only way to return to an authentic practice of Islam is to return to the ways of the *Salaf*, or "pious ancestors," who were the



contemporaries of the “rightly-guided” companions of the Prophet Muhammad.

- d. Salafists can be broken down into three different categories:
- 1) Quietists – these Salafists are internally focused, seeking to live out their Muslim faith in the most authentic way, but without attempting to change society around them.
  - 2) Activists – these Salafists proselytize (and occasionally participate in parliamentary politics) in an effort to advance the Salafist agenda (theocratic governance that emphasizes Salafist principles).
  - 3) Jihadists – Salafi-Jihadists are focused on implementing their belief system through violent means.

Salafi-Jihadists make up the principle threats we see today from international terrorists. ISIS and al-Qa’ida are Salafi-Jihadist groups.

6. Directed, Enabled, and Inspired Attacks by Salafi-Jihadist and Non-Salafi-Jihadist Organizations

- a. Directed plots occur when a violent extremist group plans specific attacks, identifies and trains operatives to affect the attack, provides financing and controls the deployment of the operatives.
- b. Inspired plots occur when a violent extremist or small group of violent extremists conduct an attack without operational contact or direct support from a terrorist group.
  - 1) The plotter(s) may declare allegiance to a terrorist group but manage all of the preparations and select the tactic, target, and timing independently.
  - 2) Terrorist propaganda and lessons learned from observing other attacks often influence those decisions.
- c. Enabled plots occur when terrorist groups provide encouragement or operational support – primarily through online communications – directly to a violent extremist or small group of violent extremists who still retain overall control of the operation.
  - 1) The attacker(s) may seek technical guidance or ideological or material support from a terrorist group, as well as recognition through coordination of media statements claiming responsibility for the attack.
  - 2) Terrorist leaders may instruct their subordinates to enable attacks by violent extremists but will not always be aware of specific plots.

The instructor will lead a discussion of the major terrorist groups including: (1) their background, origins, and history, (2) current trends, and (3) notable attacks. The content is covered below. You will need this content to complete a homework



assignment.

7. Salafi-Jihadist terrorist groups

a. Islamic State of Iraq and Syria (ISIS)

1) Background/Origin/History

a) In 2006, al-Qa'ida in Iraq led by Abu Musab Al Zarkawi (AMZ) was committing various insurgent and terrorist attacks against U.S., Coalition, and Iraqi forces during Operation Iraqi Freedom. Much of AQI's activity was conducted in the Sunni dominated Al Anbar Province, the Westernmost Province of Iraq.

(1) Though affiliated with al-Qa'ida and tacitly subject to the leadership of AQ leaders in Afghanistan and Pakistan, under AMZ, AQI conducts violent attacks which target other non-Sunni Muslims as well as military forces.

(2) This is traditionally contrary to Al Qaeda modus operandi. During that year, AMZ was killed by U.S. and Coalition forces in an airstrike.

b) Following AMZ's death in a coalition airstrike, U.S. and Coalition forces arrange a series of negotiations and cease-fires in Al Anbar Province with various Sunni Tribal Leaders.

(1) This outreach initiative, known as "the Awakening," saw the U.S. promise to build schools, hospitals, wells, and engage in other civil affairs initiatives for Sunni Muslims in Al Anbar in exchange for the Sunni tribal leaders promise to curb violent attacks against U.S. and Coalition forces.

(a) The Awakening was widely regarded as a success and led the U.S. to make a decision to withdraw the majority of its forces from Al Anbar province, to allow the Iraqi Army in that area to assume control, and for the vast majority of U.S. forces to pull back to Baghdad and eventually leave the country.

(2) As part of the U.S. draw down in Iraq and the conclusion of the period of "Awakening," the U.S. and Coalition Forces, along with the Government of Iraq, decided to issue a general amnesty for the



vast majority of people arrested and detained during the U.S. and Coalition occupation.

- (a) This resulted in a large number of detainees, held for terrorism, sectarian, and other violent activities being released and returning to their communities.
  - (b) Among these was a detainee held at the detention center in Camp Bucca Iraq. Abu Bakr Al Baghdadi.
- (3) As detainees like Al Baghdadi returned to their communities and the period of “Awakening” ended, many of these released detainees specifically Sunnis, grew disillusioned with the Iraqi Government led then by a Shiite named Nouri Al Maliki.
- (a) Maliki’s government was supported by the Government of Iran and was viewed as catering to the Shiite majority of Iraq. This sparked a new wave of Sunni extremism from nascent AQI forces. These forces were organized by Al Baghdadi under the moniker ISI, the Islamic State of Iraq.
  - (b) Circa 2010-2011, ISI (Islamic State of Iraq – former name for ISIL) struck back at Iraqi Government Forces and overran several bases securing various strongholds in Western and Northern Iraq.
- (4) In 2012, civil war broke out in Iraq’s neighbor, Syria, and threatened the regime of its Alawite President, Bashir Al Asaad.

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

- (a) Accordingly. with the Shiite backed Al Asaad struggling to maintain power, a number of Sunni extremist groups entered



Syria, along with legitimate non-sectarian rebel groups, to fight the Asaad regime. Among these was the AQ affiliated Al Nusra Front. SI (Islamic State of Iraq – former name for ISIL) used this opportunity to expand its theater of operations from Western and Northern Iraq and began operations in Syria.

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

- (b) ISI was soon the largest group among the insurgents with Nusra Front being the second. Through absorption of and , coordination and cooperation with other insurgent groups, like Nusra Front, ISI gained strength and eventually declared itself to be the Islamic State of Iraq and Al Sham (ISIS).

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

- (5) ISIS gained increased notoriety because of its social media campaign and ability to inspire ISIS affiliates in areas beyond Iraq and Al Sham. Not only was the group able to inspire Home-Grown Violent Extremists (HVEs) but it was able to undertake major attacks against western nations consisting not just of HVE activity, but concerted activities conducted by ISIS cells supported by members crossing into the west via Turkey as well as through various financing activities. Among these was the sale of oil harvested from areas under the control of ISIS fighters.
- (a) ISIS declared and imposed Sharia law in the areas of Syria and Northern and Western Iraq under its control. This included the indiscriminate killing and persecution of civilians deemed to be enemies of its faith.



- (b) In Mosul, Iraq in 2014, Abu Bakr al-Baghdadi declared himself to the Caliph of a new Caliphate established in the areas under ISIS's control. In doing so, the group adopted the moniker, ISIL, an acronym for Islamic State of Iraq and the Levant. The Levant is defined as the historic, geographic area defined as being the area south of Turkey, north of the Arabian Peninsula, and East of the Mediterranean.
- (6) In declaring its so-called Caliphate, ISIS separated territory under its control into distinct provinces called "wilayats." The majority of IS wilayats are in Iraq and Syria but with new pledges of allegiance from other extremist groups, ISIS has claimed "wilayats" in Saudi Arabia, Yemen, Egypt, Algeria, Nigeria, Libya, Afghanistan, Pakistan, Bangladesh, the Philippines, Bahrain, Tunisia, and Russia.

(b)(7)(E)

- (7) In 2017, ISIS found itself under increasing military pressure from the Iraqi Army in its occupied Iraq territory, supported by U.S. military intervention. This coupled with growing losses to the Syrian military, supported by Russia, and Coalition specific targeting, resulted in the sphere of influence of ISIS in the Levant being shrunken.
  - (a) This culminated in the battle of Raqqa, in late 2017, which saw a once major stronghold of ISIS fall.
  - (b) As a result, the group lost control of a large majority of the territory it once considered its caliphate and the group is now most commonly known as the Islamic State (IS).
- (8) By March 2018, estimates suggested that because of U.S. and Coalition strikes against IS, the territorial holdings of the group had been reduced by 98%.

## 2) Current Operational Trends

Page 2682

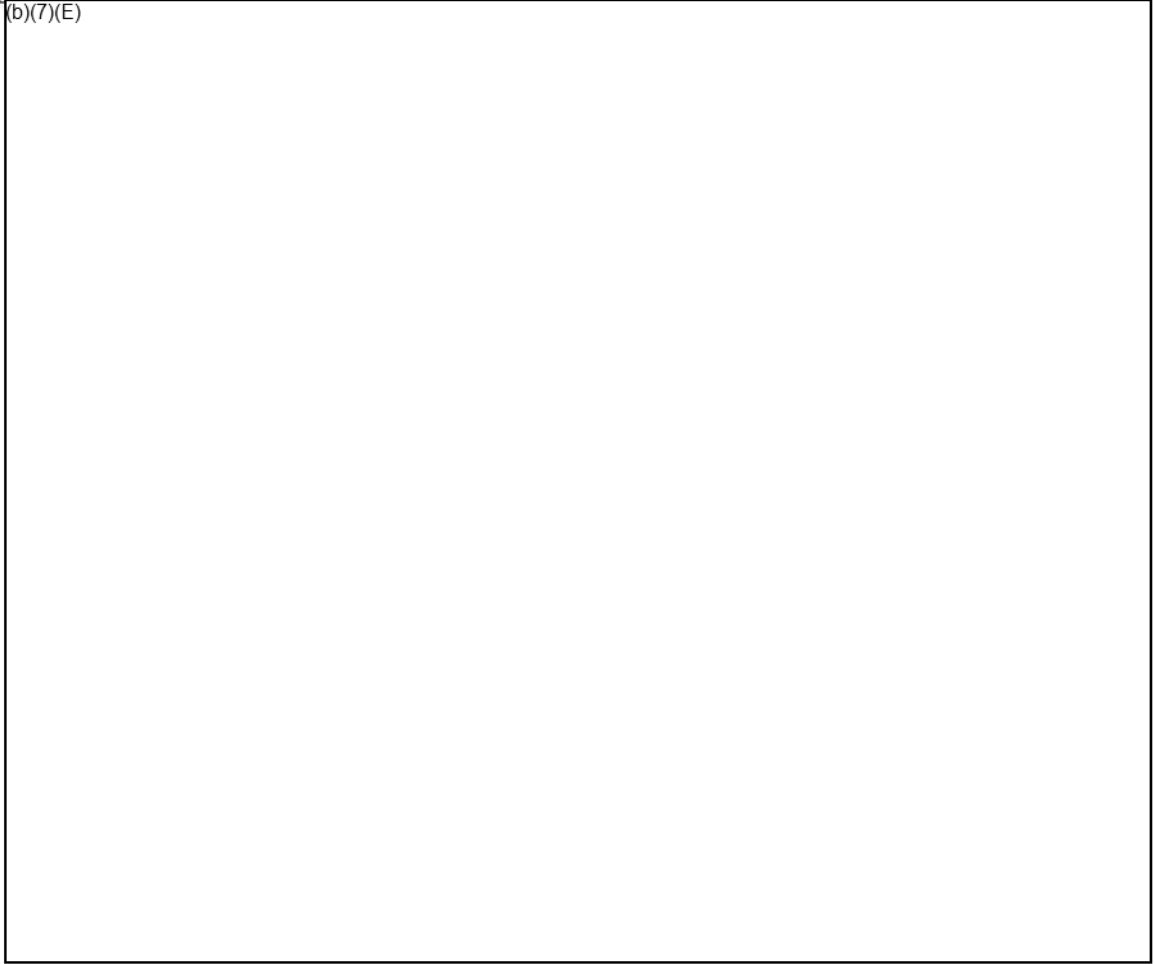
Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)



- 3) ISIS Notable Attacks and ISIS Inspired Groups/Attacks
  - a) Summer 2015 Iraq and Syria Chemical Weapons Attacks: ISISL uses chemical weapons, believed mustard agent, against targets in Syria and Iraq.
  - b) Paris Attacks – France (November 2015): Eight ISIL operatives conduct simultaneous attacks against notable civilian targets: Stade de France where an International Friendly Soccer game was being played between France and Germany (President of France was in attendance), the Bataclan Theater in Paris, and a chic restaurant section of Paris.
    - (1) One hundred thirty (130) people are killed, mostly inside the Bataclan Theater (suicide bombers at the Stade de France fail to gain entrance to the game and detonate their explosives outside of the stadium).
    - (2) The suicide bombers' devices were constructed with TATP explosive.





- c) San Bernardino Shooting (December 2015): Husband and Wife Syed Rizwan Farook and Tashfeen Malik shoot and kill 14 people at a Christmas Party at the San Bernardino Health Department.

Both were ISIS sympathizers with Farook sharing the ideology of ISIS leader Abu Bakr Al Baghdadi. and Malik having pledged allegiance to ISIS on Facebook during the shooting.

- d) Philadelphia Police Officer Shooting (January 2016): Edward Archer, a Muslim convert, ambushed Philadelphia Police Officer Jesse Hartnett by inserting his gun through the open window of Hartnett's patrol car and firing. Hartnett survived the attack and returned fire, striking Archer.

Later, Archer claimed in his interrogation that he had pledged allegiance to ISIS and carried out his attack on behalf of the group.

- e) Brussels Bombings (March 2016): ISIS operatives undertake three bombings – two bombings of the airport in Brussels and another bombing at metro station. 32 people are killed and 270 are wounded. The explosive used was TATP.

So much TATP was used that the taxi driver who drove the bombers to the airport reported smelling a noxious odor emanating from their luggage.

- f) Bastille Day Lorry Attack - France (July 2016): Mohamed Lahouaiej-Bouhlel, a Tunisian-French citizen, drove a truck through a crowd in Nice, France during evening celebrations of Bastille Day. 84 people were killed and over 300 were injured.

- g) Las Ramblas Lorry Attack – Spain (August 2017): Five (5) attackers affiliated with ISIS drove a van into crowds of people on the Las Ramblas pedestrian walkway in Barcelona, Spain. The day after, the attackers attempt to run over a crowd of people in the resort town of Cambrils, Spain (south of Barcelona). 16 people are killed and over 130 are injured in the two attacks.

**Note:** Authorities later determined that an explosion at a house in a town outside of Barcelona was linked to the attacks; specifically, investigators believed the Las Ramblas attacks was to involve explosives and the residential explosion was caused by the making of explosives by three additional members of the



conspiracy – all of whom were killed in the blast)

- h) Christmas Market Lorry Attack – Germany (December 2016): An ISIS sympathizer of Tunisian descent, Anis Amri, drove a truck through a Christmas market in Berlin, Germany. The attack killed 12 people and injured 48 more.

Amri used the messaging application, Telegram, to maintain contact with ISIS operatives in Libya.

- i) London Bridge Attack - Great Britain (June 2017): Three ISIS affiliated attackers, Khuram Shazad Butt (British Citizen born in PAK), Rachid Redouane (Moroccan- Libyan National), and Youssef Zaghba (Moroccan-Italian National) conducted a vehicle attack on London Bridge, running over pedestrians, ultimately killing 3 people. After crashing the vehicle, the three attackers began slashing and stabbing people in a local market/pub district with ceramic knives. The three were also wearing fake suicide bomber vests. Eight people were killed in total.

Post-mortems on all three attackers revealed the attackers had taken large quantities of steroids prior to the attack.

- j) London Westminster Attack – Great Britain (March 2017): Khalid Masood, a 52-year old Briton and ISIS sympathizer, conducted a vehicle and edged weapon attack that resulted in the deaths of 5 people. Specifically, Masood ran over four people in a rental car on Westminster Bridge and, after crashing, approached the gates of the British Parliament on foot and stabbed a police officer to death.

A post-mortem of Masood similarly established use of anabolic steroids prior to the attack.

- k) Manchester Arena Bombing - Great Britain (May 2017): Salman Abedi, an ISIS operative and suicide bomber, detonated an improvised explosive device (IEDs) outside of an Ariel Grande Concert in Manchester, England. Abedi was a UK citizen born to a family of Libyan origin. Abedi targeted civilians, specifically young female adults and teenagers, as they departed the concert venue. 22 people were killed. Abedi, along with his brother Hashem Abedi, were believed to have joined ISIS in 2015. Abedi himself is believed to have been connected to ISIS External Operations Brigade Commander Katibat Al-Battar Al Ibi (whose brother was the commander of the ISIS Paris 2015 Attacks).



- (1) Attack was planned for approximately one year and was a classic “lone wolf” attack in that Abedi carried out the entire operation from planning to deployment without assistance.

Authorities established Abedi had previously traveled from England to Libya in the months prior to the bombing where they believed he received training in the making of explosives.

- (2) This was supported by evidence regarding the device recovered from the scene: TATP as the explosive, detonator assembly was correct, and shrapnel was packed evenly in the device. Abedi was also under surveillance by intelligence and security authorities while in Libya.
- l) Pulse Night Club Shooting (June 2016): Omar Mateen, a USC, shoots and kills 49 people and wounds another 53 at a gay nightclub in Orlando, FL. During the attack, Mateen called 911 and pledged allegiance to ISIS and Abu Bakr Al Baghdadi. ISIS claims responsibility for Mateen’s actions via its Amaq News Agency, using its Telegram messaging channel, and via its Al Bayan radio station.

**Note:** This demonstrates the strength and depth of ISIL’s propagand network and their ability to leverage multi-media platforms.

- m) Mall Attack in St. Cloud, Minnesota (September 2016): Dahir Adan, a U.S. resident, conducted a stabbing spree at a mall in St. Cloud, MN injuring 10 people.
- n) Ohio State Attack – Ohio (December 2016): Abdul Razak Ali Artan, a U.S. resident and ISIS sympathizer, conducts a car and knife attack on the campus of Ohio State University in Columbus, Ohio. The attack results in the wounding of 11 people.
- o) New York Central Park Lorry Attack (October 2017): Sayfullo Habibullaevic Saipov, an Uzbek national residing in the U.S., conducts a vehicular attack in New York City by driving his truck down a bike path. Saipov claims ISIS inspiration. Eight people are killed, and more than 12 people are injured.
- p) New York Port Authority Attempted Bombing (December 2017): Akayed Ullah, a Bangladeshi national living in the U.S., attempts an attack on the Port Authority Bus Terminal in New York City. Specifically, Ullah detonated a pipe bomb under the terminal which malfunctioned and



only injured Ullah who had previously declared allegiance to ISIS.

(b)(7)(E)

b. Katibat al-Battar al-Libi (KBL)

1) Background/Origin/History

- a) Founded by Libyan Jihadists; the group recruited and trained Libyan and Tunisian fighters who then went to fight in the Syrian civil war for KBL in alignment with ISIS.
- b) Pledged allegiance to ISIS and Abu Bakr Al Baghdadi in 2014 when Al Baghdadi declared himself to be Caliph for a new Caliphate.
- c) Soon after this pledge of allegiance, KBL established the first Libyan Islamic State Wilaya.

2) Current Trends

a)

(b)(7)(E)

b)

3) Notable Attacks

- a) Besides the connections KBL has had to ISIS attacks and plots in Europe, specifically the training of operatives, the group has launched attacks in North Africa using its Libyan hubs.

- (1) Bardo National Museum – Tunis (March 2015): three Tunisians shot 22 people, mainly Western tourists in an attack on the museum. The gunmen were identified as an ISIS cell.



- (2) Sousse Beach Resort – June (2015): A Tunisian, Seifidine Rezgui, kills 38 people (30 UK Citizens) on the beach at a resort hotel in Sousse. Rezgui was identified as having close links to the ISIS cell who undertook the Bardo National Museum attack.
- c. ISIS – Khorasan (ISIL-K)
- 1) Background/Origin/History
    - a) Formed in 2014 after six former senior members of the Tehrik-e-Taliban Pakistan pledged allegiance to IS Leader Abu Bakr al Baghdadi.
    - b) Estimated membership varies greatly with as low as 1,500 up to 11,500; recruits form disaffected former Taliban members.
  - 2) Current Trends
    - a) 

(b)(7)(E)
  - 3) Notable Attacks
    - a) The group carries out suicide bombings, small arms attacks, and kidnappings in Afghanistan against civilians as well as Afghan security and defense forces; the group has also claimed responsibility for attacks on civilian targets in Pakistan.
- d. Al-Qaeda
- 1) Background/Origin/History
    - a) Al Qa'da (AQ) was formed in 1988, during the latter stages of the Soviet-Afghan war, by Osama Bin Laden. It is a Pan-Islamist, Sunni terrorist group formed with the goal of waging a global jihad and to fight back against the perceived imperialism of Western nations in the Muslim world. As such, the group adheres to the ideologies and doctrines found in Salafism, Qutbism, and Takfirism.
    - b) AQ is a jihadist network that seeks to establish a caliphate, a global Muslim State, which operates under Sharia (Islamic) law. There are three cornerstones of AQ's doctrine:
      - (1) Unite the world's Muslim population under Sharia law.



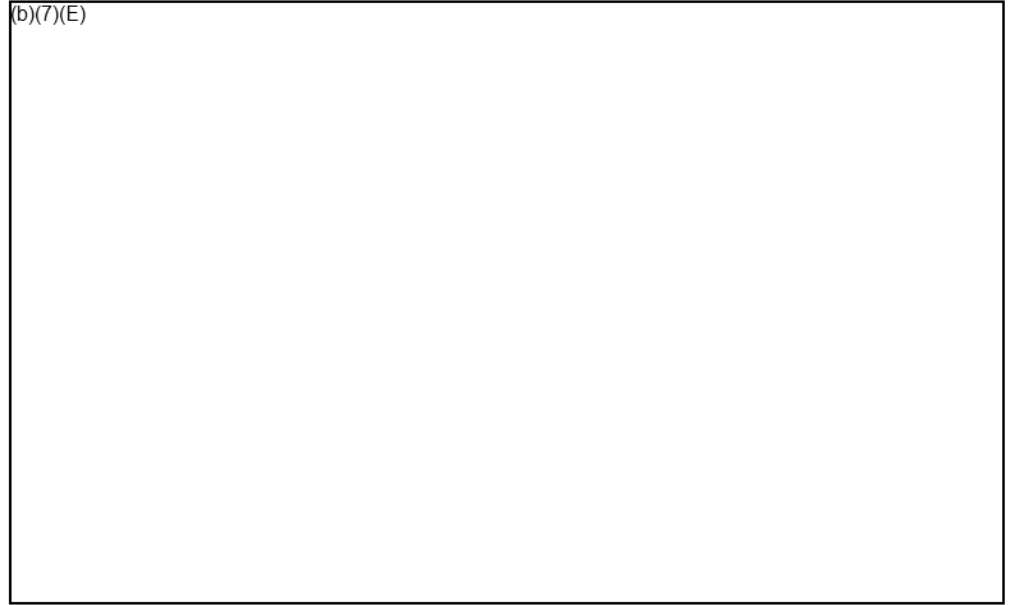
- (2) Liberate the “Holy Lands” from the “Zionist-Crusader” forces (Israel and the United States).
  - (3) Alleviate perceived economic and social Injustices.
- c) AQ views itself as fighting a defensive jihad (contrasted with ISIL which views itself as fighting an offensive jihad).
- d) Ultimately, AQ believes that it is fighting a “defensive jihad” against the United States and its allies, defending Muslim lands from the “new crusade led by America against the Islamic nations.”
- (1) In his 1996 declaration of jihad against the United States, Osama bin Laden justified the use of force by citing 13th century Islamic scholar Ibn Taymiyyah: “To fight in defense of religion and Belief is a collective duty; there is no other duty after Belief than fighting the enemy who is corrupting the life and the religion. There [are] no preconditions for this duty and the enemy should be fought with [one’s] best abilities.”
- e) Structure
- (1) AQ’s central command is headquartered in Afghanistan and Pakistan. AQ’s current leader is Ayman al-Zawahiri (Osama Bin Laden’s deputy until Bin Laden was killed in a U.S. assault in 2011.)

(b)(7)(E)



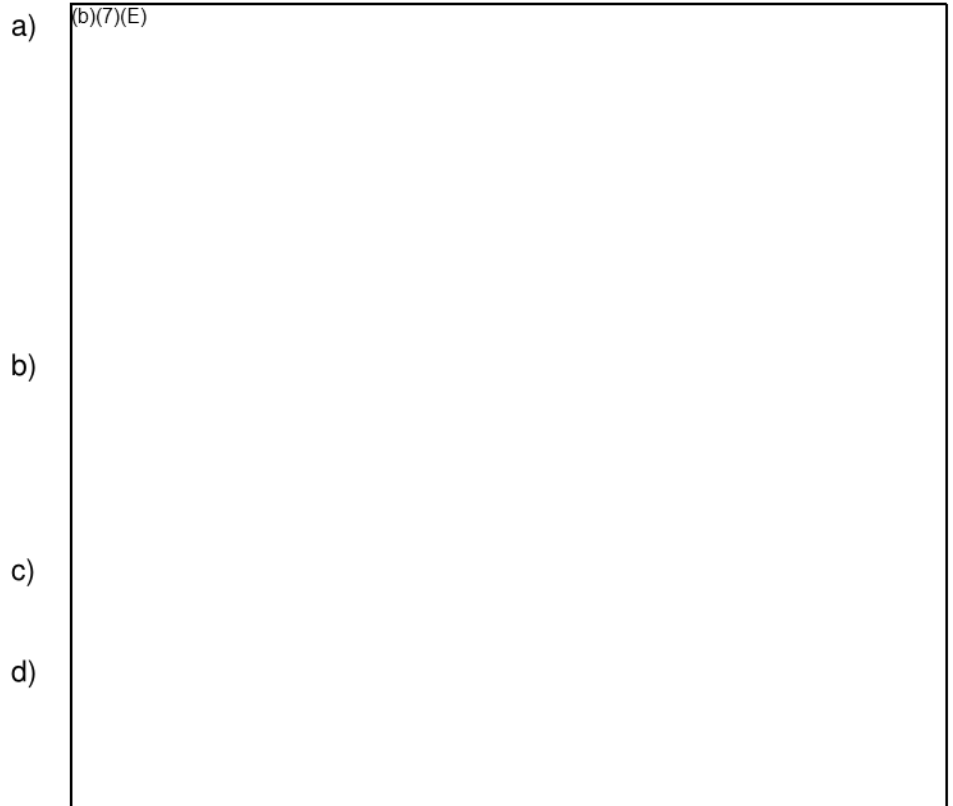


(b)(7)(E)



2) Current Operational Trends

a) (b)(7)(E)



b)

c)

d)

3) Notable Attacks:

a) September 11, 2001 (9/11) Attacks:

- (1) 19 AQ operatives hijacked four U.S. commercial flights and flew two of into both towers of the World



Trade Center and another in the Pentagon. A fourth plane crashed in Pennsylvania after being hijacked when passengers on board attempted to retake the aircraft. Over 3,000 Americans were killed in the deadliest terror attack in U.S. history.

- b) 1998 U.S. Embassy Bombings in Africa
  - (1) AQ operatives conducted simultaneous suicide bombings against the U.S. Embassies in Dar es Salaam, Tanzania and Nairobi, Kenya. As a result, 258 people are killed and over 5,000 wounded.
- c) 2002 Attempted “Dirty-Bomb” attack on U.S.
  - (1) Jose Padilla, aka Abdullah al-Muhairi, a U.S.C., was arrested at Chicago’s O’Hare International Airport after arriving on a flight from Zurich. Al Muhairi had traveled to Pakistan and Afghanistan, following his conversion to Islam, and discussed the bomb plot with AQ leaders. A captured AQ leader provided information concerning al-Muhairi to U.S. intelligence. Al-Muhairi met with AQ leaders regarding a plan to acquire and detonate a radiological device aka a “dirty bomb.”
- d) November 2002 Bombing in Mombasa, Kenya
  - (1) AQ operatives bombed a hotel in Mombasa frequented by Israelis, killing 15 and wounding 40. AQ operatives, on the same day, attempt to shoot down an Israeli airliner on take-off from Mombasa’s airport with a surface-to-air missile.
- e) 2004 Madrid Train Bombings
  - (1) Four rush-hour commuter trains in Madrid were attacked simultaneously by AQ operatives using explosives in back-packs detonated remotely via mobile phones. 191 people are killed and over 1,800 wounded. Among the perpetrators were individuals of Moroccan, Syrian, Egyptian, Algerian, Lebanese, and Spanish descent.
- f) 2005 London Underground Bombings
  - (1) AQ operatives conduct suicide bombings on a London Underground station and bus. The attacks, perpetrated by four British Nationals, killed 56





people in what became the worst terrorist attack in UK history. Later in that month, AQ operatives, all British Nationals, attempted to blow up three commuter trains and a bus in London but the bombs failed to detonate.

- g) 2006 Transatlantic Aircraft Pilot
  - (1) A group of British men who were allegedly in contact with AQ leaders began plotting to carry-out the near-simultaneous detonation of peroxide-based liquid explosives by suicide bombers on as many as 18 transatlantic flights bound for the U.S. and Canada. The plot was disrupted by Britain's MI5 and the FBI and resulted in the ban on carry-on liquids on commercial aircraft.

**Notes:**

**AQ Affiliates**

- e. Al Qa'da in the Arabian Peninsula (AQAP)
  - 1) Background/Origins/History
    - a) AQAP, like its parent AQ, is a Sunni jihadist group which follows an ideological strain of Qutbist, Salafist, and Takfiri



thought. The group was formed in 2009 from the merging of AQ affiliated groups in Saudi Arabia and Yemen.

- (1) As with the broad AQ mandate, AQAP declared its intention to establish an Islamic Caliphate and implement Sharia law.
- b) Many of AQAP's leaders and founders have strong ties to AQ and Osama bin Laden.
  - (1) Many traveled to Afghanistan in the late 1990's and early 2000s to train at AQ camps.
  - (2) In addition, eventual AQAP leaders were identified as being involved in the bombing of the USS Cole in 2000.
- c) Since the union of AQ branches in Saudi Arabia and Yemen under the banner AQAP, the group has carried out violent jihadist attacks both domestically and internationally in service of Al Qa'ida's ideology.
  - (1) Although the group carries out most of its attacks inside Yemen, AQAP is widely known for carrying out the fatal shooting at the Paris offices of French satirical magazine *Charlie Hebdo* in January 2015, as well as for its involvement in terrorist plots on U.S. soil, including the "Christmas Day Bomber" in 2009 and the "Times Square Bomber" in 2010.
- d) In 2012, following removal of Yemeni President Ali Abdullah Saleh from office, AQAP took advantage of the fractured political scene by establishing an insurgency in southern Yemen.
  - (1) Since Yemen descended into civil war in 2015, AQAP has benefited from the political vacuum by attempting to develop its own pseudo-state in the southern region.
  - (2) The civil war has coincidentally strengthened AQAP by causing Western forces to withdraw and the Yemeni and Saudi Arabia forces to focus on the opposing Houthi rebels.
  - (3) AQAP has developed a pseudo-state in the southern region of Yemen.
- e) The struggle between Iran backed Houthi rebels and the Saudi Arabia supported Yemeni forces, has resulted in AQAP being strengthened by virtue of the vast amount of support being given to anti-Houthi forces.



Anti-Houthi forces regularly enter into alliances with AQAP and turn a blind eye to the group's terrorist activities.

- f) Support for AQAP extends to the highest levels of Yemen's Government. In fact, several associates of the Saudi-backed President Mansour al-Hadi have appeared on a U.S. Treasury list of global terrorists for allegedly providing financial support to, and acting on behalf of, AQAP.
- g) AQAP operates throughout Yemen, primarily in the country's southern and central regions. In many of these provinces, AQAP governs small pockets of territory with sharia (Islamic law) courts and a heavily armed militia. AQAP attempts to appeal to the Yemeni people by meeting their basic needs and integrating into the local population, including by conforming to the local governance structures.
  - (1) According to a February 2017 report by the International Crisis Group, AQAP has successfully presented itself as "part of a wider Sunni front against Houthi expansion," further providing the organization with local allies and room to operate in the country.
- h) In addition to controlling large parts of Yemen, AQAP poses a significant terrorist threat to Western Countries, including the United States. Specifically, the group has conducted and attempted to conduct numerous terrorist operations worldwide.
- i) In 2012, additional AQAP objectives were enunciated which declared the group's primary goals to be:
  - (1) The expulsion of Jews and Christians from the Arabian Peninsula
  - (2) The establishment of the Islamic Caliphate and Sharia rule in areas currently governed by "apostate" governments in the region
- j) AQAP champions a violent interpretation of "Jihad." In doing so the group encourages Muslims to hate the people of the West and to indoctrinate that hatred and "love of jihad" in their children.

AQAP is believed to be the AQ affiliate most ideologically similar to AQ's core tenets.

- k) Structure



- (1) AQAP is hierarchal and has a strong division of labor. There is a political leader in charge of overall direction of the group, a military chief, and a propaganda wing that engages in recruits, provides justifications for attacks, and provides spiritual guidance. This structure too mirrors AQ proper.
  - (a) AQAP 's political leader is one of its co-founders, Qasim al-Raymi. Raymi took control following the death of his predecessor in a U.S. drone strike.
  - (b) AQAP's military branch plans all of its violent attacks and insurgent activities against the Yemeni Government and military. Ibrahim al-Asiri is AQAP's chief bomb-maker and is responsible for the group's most high-profile bombing attempts – 2009 Christmas Day Bomber and 2010 Times Square Bomber.
  - (c) Propaganda for AQAP is conducted via its recruiters and publications which includes a media channel called "*Al-Malahem.*" Al-Malahem publishes a bi-monthly magazine in Arabic for Yemenis and the notorious English language magazine, *Inspire*, directed at its American audience.
  - (d) In addition, AQAP publishes a digital newsletter, *al-Masra*, which includes news and updates on the entire AQ network.
    - i. Inspire magazine provides answers to questions about AQAP and its mission.
    - ii. The magazine also has provided tips for bomb-making including making Vehicle Borne Improvised Explosive Devices (VBIEDs) and bombs unable to be detected by airport security systems.
    - iii. The magazine has also published a list of targets for supporters, sympathizers, and lone-wolves to attack in the west.
    - iv. The magazine has expanded AQAP's reach to people well beyond the Arabian peninsula and to people who don't speak Arabic.



v. AQAP has also used social media sites its advantage; the group, despite having numerous accounts shut down, continues to have a standing presence on Twitter.

(b) Anwar al-Awlaki was a well-known, American-born, AQAP recruiter who was linked to the 2010 Fort Hood shooter, U.S. Army Major Nidal Hassan; the shooting resulted in the deaths of 13 soldiers. Al-Awlaki also had contact with AQAP operative and Charlie Hebdo attacker Cherif Kouachi. Al-Awlaki was killed in a U.S. drone strike in Yemen in 2011.

## 2) Current Trends

a) AQAP finances its activities through robberies and kidnap/ransom operations. "Hostages" have been referred to be the group as a "profitable trade and a precious treasure."

(1) AQAP also participates in gun and drug smuggling which has included trafficking opium.

(2) AQAP also reportedly generated millions of dollars through the duration of its control of Yemen's third largest port; the group imposes taxes and tariffs on passing and entering vessels.

(3) The group also looted the central bank branch in Mukalla, netting an estimated \$100 million USD. Finally, AQAP gets funding through donations from like-minded supporters, mostly in Saudi Arabia.

b) AQAP is currently competing for recruits with ISIS who established an affiliate in Yemen in 2015. AQAP has raised its recruiting standards, especially for those coming from the West. AQAP has also tried to inspire potential recruits to remain in their home countries and undertake attacks rather than traveling to fight in Yemen.

c) AQAP has published and disseminated a previously composed training guide called the "Encyclopedia of Jihad" (available on the internet as of 2003); the encyclopedia is a collection of texts which provide information on:

(1) Making explosives

(2) Using pistols, grenades, mines, artillery, machine guns, and armor-piercing weapons

(3) Espionage



- (4) Security precautions
  - (5) Use of compasses
  - (6) How to read maps
  - (7) Acts of sabotage
  - (8) Secure communication
  - (9) Reconnaissance
- 3) Notable Attacks/Operations
- a) Charlie Hebdo (Paris) – January 2015
    - (1) Charlie Hebdo is a satirical magazine which began publishing in 1970. The magazine satirizes religion, politics, and other topics.
    - (2) In 2006, the magazine re-printed controversial cartoons of the Prophet Mohammad which originally appeared in a Danish Newspaper.
    - (3) In 2011, the satirical publication was firebombed after naming the Prophet Muhammad as its “editor-in-chief.”
    - (4) Main attackers were brothers Said Kouachi and Cherif Kouachi (Known / Suspected Terrorists (KSTs) and on the no-fly list) were affiliated with AQAP and spent time in Yemen receiving weapons and other training from the group.
      - (a) **(Note:** A third attacker, Amedy Coulibaly, claimed allegiance to ISIS before being killed by police).
      - (b) The attackers, armed with guns and bulletproof vests, forced their way into the Charlie Hebdo office in Paris at approximately 1130 hours and kill 12 people.
    - (5) Over the next two days, the Kouachi brothers and Coulibaly kill two additional police officers (one police officer was one of the initial 12 people killed at the magazine). The Kouachi brothers and Coulibaly take hostages and stand-off with police in two different locations in France. Ultimately all three attackers and some of the hostages are killed.

AQAP openly claimed responsibility for the attack.
    - (6) 2010 “Times Square Bomber” – the perpetrator, Faisal Shahzad, a Pakistani-born naturalized U.S.C., parked an SUV loaded with homemade



explosives in New York's Times Square. The bomb failed to detonate (reportedly due to an incorrectly set timer) and he was subsequently arrested at JFK while on board a flight to Dubai.

(a) Initially thought to be affiliated with the Pakistani Taliban, Shahzad had aligned himself with the Pakistani Taliban (TTP) but was also found to have drawn inspiration from Anwar Al-Awlaki.

(7) 2009 "Christmas Day Bomber" – the perpetrator, Umar Farouk Abdulmutallab, a Nigerian, attempted to detonate plastic explosives aboard a Northwest Airlines Flight from the Netherlands bound for Detroit. Abdulmutallab, known euphemistically as the "underwear bomber" told authorities he was in contact with Al-Alwaki via the internet and that he spent a month at a training camp in Yemen, north of Sanaa, receiving training from an AQ bombmaker.

f. Al-Qa'ida in the Islamic Maghreb (AQIM)

1) Background/Origins/History

a) AQIM, like AQ at large, is a Sunni jihadist group which follows an ideological strain of Qutbist, Salafist, an Takfiri thought. It is also known as *Jamaat Nusrat al-Islam wal Milimeen* (JNIM) which name began to be used following merger between AQIM and local, smaller salafist groups in the region. Despite this, the group still identifies as AQIM and is under the direction of AQ.

b) AQIM was first founded in Algeria; its predecessor organization was known as Le Groupe Salafiste Pour La Predication Et Le Combat (GSPC) also known as the "Salafist Group for Preaching and Combat."

(1) The GSPC was born in 1998 as a splinter group from the Armed Islamic Group.

(2) The group's stated goal was the overthrow of the Algerian Government. Specifically, the founders of AQIM include Hassan Hattab and Abdelmalek Droukdel, both former leaders of GSPC. GSPC merged with Al Qaeda (and became AQIM) in 2007.

2) Current Trends



- a) AQIM continues to be based in North Africa and has extended its operations from Algeria to the Cote d'Ivoire, Mali, Niger, Libya, Mauritania, and Tunisia. The group reportedly operates training camps in northern Mali.
- b) AQIM seeks to institute Sharia law in all of its areas of operations, much as AQ. The group sees secular governments in North Africa as apostates left over from European colonialism and, as such, illegitimate.
- c) AQIM sustains itself through proceeds gained from kidnapping and extortion. Funds are also raised through protection rackets, robbery, people and arms trafficking, money laundering, smuggling, and the facilitation of drug trafficking from South America to Europe.
- d) AQIM also engages in global fundraising operations; this includes support garnered from individuals located in Western Europe who provided financial and logistical support.

AQIM is also believed to receive support from foreign governments, including Iran and Sudan, and AQ at large which provides further material and financial support.

- e) AQIM is believed to have recruited several fighters from Abu Musab Al Zarqawi's AQI and, as its operations have spread outward from Nigerian, in particular in Mali, Niger, and Cote d'Ivoire, has recruited a large number of sub-Saharan Africans to its ranks.
- f) AQIM leadership has long standing ties to AQ and its deceased leader and founder, Osama bin Laden.
- g) AQIM has reportedly sent fighters to train with Hezbollah in Lebanon and furnished technical assistance to Boko Haram fighters in the manufacture of Improvised Explosive Devices (IEDs). AQIM's assistance to Boko Haram also has reportedly included weapons and funding.

3) Notable Attacks/Operations

- a) August 2017: AQIM attacks a restaurant in Burkina Faso killing 18 people and, on the same day, carries out attacks against U.N. Peacekeeping troops in two different locations in Mali.
- b) March 2016: AQIM attacks a beach resort in Grand-Bassam, Cote d'Ivoire.
  - (1) It is the first AQ attack in the country and results in 19 people killed including various foreign nationals from Germany, France, Mali, Cameroon, and Burkina Faso (landlocked West African nation bordered by Mali and Cote d'Ivoire).





- c) January 2016: AQIM stages simultaneous attacks on a hotel and police station in Burkina Faso; 30 people from 18 different nations are killed.
- d) November 2015: AQIM carries out an attack on the Radisson Blu Hotel in Mali in which, during the attack and subsequent hostage-taking, 21 people were killed.

The perpetrators used counterfeit diplomatic license plates to gain access to the hotel.

- e) July 2014: French Authorities foil AQIM plot targeting the Eiffel Tower, the Louvre, and a French nuclear power plant.
- f) September 2012: Attack on the U.S. Embassy in Benghazi, Libya by Ansar al-Sharia (AAS) which resulted in the killing of U.S. Ambassador J. Christopher Stevens.

AQIM reportedly linked to the planning of the attack and command and control links to AAS fighters who carried out the attack.

- g) November 2011: AQIM kidnapped seven people – all foreign nationals from France, Sweden, the Netherlands, and South Africa – from a Uranium Compound in Niger.
- h) September 2010: AQIM kidnapped five French Nationals working for a Nuclear Company in Niger.

g. Al-Qa'ida in the Indian Subcontinent (AQIS)

1) Background/History/Origins

- a) Founded in 2014 by AQ leader Ayman Al-Zawahiri
- b) Like AQ proper, AQIS follows a Salafist ideology with a central tenet of waging “physical jihad” to impose sharia law and establish a caliphate in the Indian subcontinent. To that end, AQIS is active not just Afghanistan and Pakistan but in India, Burma, Bangladesh (AQIS branch referred to a Ansar al Islam), and Kashmir.

2) Current Operational Trends

(b)(7)(E)



c)

(b)(7)(E)

d)

e)

f)

3) Notable Attacks

a) September 2014 Attempted Seizure of Pakistani Navy Frigate

- (1) AQIS operatives attempted to seize control of a Pakistani Navy Frigate from which they planned to fire missiles at American and other Pakistani vessels. The operation involved a small arms attack and a suicide bomber.

h. Al Shabaab

1) Background/Origins/History

- a) The group's name translates to "the Youth."
- b) Sunni extremist group founded in 1996-1997 in Somalia by Ibrahim Hai Jaama' Al Afghani; the group grew out of the rebel group which fought with the Somalia regime during the Somali Civil War of the early 1990s. **(Note:** Its precursor was the extremist group al-Itihad al-Islami [AIAI aka Unity of Islam]).

- (1) The group's original goal was to establish a "Greater Somalia" under sharia law. The group fought a guerilla campaign against Ethiopian occupation after Ethiopia, supported by the U.S. invaded Somalia and drove Islamist forces out of Mogadishu.
- (2) The Ethiopian occupation ended in 2008; the group has continued to target Ethiopians and Kenyans,



specifically, for its planned attacks outside of Somalia.

- c) The group's ideology adheres to many of the radical Islamic doctrines; chiefly, Wahabism, Salafism, Qutbism, Takfirism.

The group seeks to establish an Islamic caliphate inside Somalia that will eventually grow to encompass the entire Horn of Africa.

- d) Al Shabab supports "Takfir" which advocates the ex-communication of apostates, treats them as non-believers, and is used to justify their killing.
- e) The group operates in Somalia, Kenya, Ethiopia, and Djibouti and is Al Qaeda's formal affiliate in East Africa; pledged allegiance to Al Qaeda in 2012.

## 2) Current Operation Trends

(b)(7)(E)



f)

(b)(7)(E)

3) Notable Attacks

- a) Muna Hotel Attack – Mogadishu (August 2012): Al Shabaab gunmen attack the Muna Hotel disguised as security personnel. The resulting two-hour gun battle and suicide bombing kills 32 people including several members of the Somali parliament.
- b) Westgate Shopping Center Attack – Nairobi, Kenya (September 2013): Al Shabaab operatives raided the Westgate Shopping Center in Nairobi, Kenya. The shopping center was known to be heavily frequented by Westerners.
  - (1) During the attack and ensuing four-day stand-off, 67 people were killed and over 200 wounded.
  - (2) During the attack and stand-off, Al-Shabaab militants would ask victims if they were Muslim and had victims prove it by reciting verses of the Quran. Those who disclaimed being Muslim or who could not recite the Quran were executed.
- c) Somalia Presidential Palace Attack – Mogadishu (February 2014): Al-Shabaab militants attack the Somali Presidential Palace with a combination of vehicle borne improvised explosive devices (VBIEDs) and small arms. Fourteen people are killed including nine of the attackers.
- d) Truck Bomb Mogadishu City Center (October 2017): An Al Shabaab militant detonated a Truck VBIED in downtown Mogadishu killing between 320 and 587 people. It was Somalia's worst terrorist attack to date.

8. Prominent Non-Salafist Islamist Terrorist Groups

- a. Hezbollah (translation: "The Party of God")
  - 1) Background/Origins/History
    - a) Shi'a Extremist Group created with the help of Iran in the early 1980s under the pretense of fighting foreign



occupiers in Lebanon which refuses the right of the Jewish State of Israel to exist

- b) Active in Terrorist Attacks against Israelis, the Jewish State of Israel, as well as American and Jewish targets around the world
- c) Hezbollah resembles a proxy force for the Government of Iran (GOI) and receives funding, training, and weapons through the Islamic Revolutionary Guard Corps (IRGC).
- d) Consists of a Political Wing and an Armed Wing. Since 1992, Hezbollah has had a presence and large influence in the Lebanese elected government.

- (1) The European Union has designated the Armed Wing a Terrorist Organization.
- (2) The Political Wing of Hezbollah was specifically exempted from this designation.

2) Current Trends

(b)(7)(E)

3) Notable Attacks

- a) Responsible for the 1983 US Marine Barracks bombing in Beirut; believed to be supported in the attack by Iran and Syria. The attack resulted in the deaths of 241 service members.
  - (1) 2003: US District Court Judge finds that Hezbollah carried out the attack at the direction of the Iranian Government.
  - (2) 2007: US District Court orders Iran to pay \$2.65 Billion USD to Survivors and family members of service members killed in the 1983 bombing.
  - (3) 2010: Lawsuit filed in New York City seeking to force the Iranian Government to pay the \$2.65 Billion USD awarded in 2007.
  - (4) 2012: Judgment for \$2.1 Billion USD formally issued by U.S. District Court against Iran.
  - (5) 2013: US District Court issues ruling to release \$1.75 Billion of Iranian funds, frozen in a New York Citibank Account, to set up a fund for victims of the 1983 bombing.
  - (6) 2014: Federal Appeals Court affirms both the judgment against Iran and the release of the \$1.75 Billion USD.



- (7) 2016: US Supreme Court Affirms and rules the survivors and families of the 1983 bombing victims should be allowed to collect the \$1.75 Billion USD.

9. Boko Haram

a. Background/Origins/History

- 1) Official Arabic Full Name: Jama'atu Ahlis Sunna Lidda'awati wal-Jihad
  - a) Translates as "People Committed to the Propagation of the Prophet's Teachings and Jihad"
  - b) "Boko Haram": Literal Translation from Arabic means "Fake is Forbidden."

Commonly understood translation from Arabic is  
"Western Education is Forbidden"

- 2) Formed in 2002 in Nigeria (Africa's most populous nation) by a Salafist cleric named Mohammed Yusuf.
- 3) Based in Maiduguri in Northeastern Nigeria
- 4) Focused on opposing western education and establishing a caliphate in Nigeria.

The group operates in Nigeria, Cameroon, Chad, and Niger.

- 5) Conducted attacks on Nigerian military and security forces and engaged in wholesale kidnappings of children, often girls. Most famously, conducted a 2013 kidnapping of 200 school girls from a town in Nigeria which captured the world's attention and condemnation.
  - a) The group also kidnaps school age boys to turn them into Boko Haram fighters. Declared a caliphate in the areas of Nigeria it controlled in 2009 (Islamic State of West Africa Province – ISWAP) and engaged in violence against the Nigerian government following the Government's killing of Yusuf.
  - b) In 2014, the Nigerian military pushed Boko Haram back into its regional area of Northeastern Nigeria.
- 6) Boko Haram fighters are distinguishable by their facial scars and heavy Hausa accents which make them readily identifiable to other Nigerians.
- 7) Affiliated with the Islamic State of Iraq and Al Sham (ISIS). Prior to this affiliation, Boka Haram maintained ties to AQIM. Various Boko Haram members had previously trained and fought with AQIM in Mali.



- a) Leader is Abubakar Shekau.
- b) In August 2016, ISIS recognized another individual as Boko Haram's leader, Abu Musab Al Barnawi.

This has factionalized Boko Haram as Shekau and Al Barnawi fight for control of the group.

b. Current Operation Trends

(b)(7)(E)

c. Notable Attacks

- 1) Chibok Kidnapping – Borno State (April 2014): Boko Haram kidnapped over 200 girls from a school in Chibok, Nigeria. This



- kidnapping triggered international condemnation and the “Bring Back Our Girls” social media campaign.
- 2) Kidnapping of the Wife of the Cameroon Vice Prime Minister (July 2014): Amadou Ali, a prominent Cameroon political figure and spouse to the Vice Prime Minister is kidnapped by Boko Haram militants and subsequently released three months later along with 27 other hostages, presumably in exchange for a ransom paid by the Cameroonian Government.
  - 3) Nigerian Town Seizures (August 2014): Boko Haram begins attacking and seizing towns in Nigeria in an attempt to take and hold territory in furtherance of the establishment of its own Islamic State.
  - 4) Children Burned Alive (February 2016): Boko Haram kills and burns 86 children alive in response to perceived provocation from the Nigerian Government.
  - 5) Elementary School Attack – Damasak (November 2016): Boko Haram militants kidnap approximately 400 people, at least 300 of which are elementary school students.

**Notes:**

**F. EPO 6: Recognize risk factors and indicators of radicalization and mobilization.**

1. Homegrown violent extremists (HVEs)
  - a. Persons of any citizenship who have lived and/or operated primarily in the U.S. or its territories who advocate, engage in, or prepare to engage in ideologically-motivated terrorist activities (to include providing support to terrorism) in furtherance of political or social objectives promoted by a





foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization.

(b)(7)(E)

- b. HVEs can be classified as either “inspired” or “enabled” by foreign terrorist organizations (see above discussion concerning directed, enabled, and inspired).

- 2. Based on a historical analysis of HVE events by an Interagency Analytic Focus Group formed by the National Counterterrorism Center, the following observable behaviors have been identified as possible indicators of an individual's preparation to engage in violent extremist activity. (b)(7)(E)

(b)(7)(E)

- a. Group A Indicators (b)(7)(E)

- 1) (b)(7)(E)
- 2)
- 3)
- 4)
- 5)

- b. Group B indicators (b)(7)(E)

- 1) (b)(7)(E)
- 2)
- 3)
- 4)
- 5)
- 6)
- 7)
- 8)
- 9)
- 10)



(b)(7)(E)

c.

Group C Indicators

(b)(7)(E)

(b)(7)(E)



- 13)
- 14)
- 15)
- 16)
  
- 17)
- 18)
- 19)
  
- 20)

(b)(7)(E)

**Notes:**

[Redacted Notes Area]

**THIS ENDS SESSION 1**



**Class Assignment**

(b)(7)(E)

**SESSION 2**

**Class Assignment Presentation**

(b)(7)(E)

- G. EPO 7: Describe the United States' national security architecture and a HSI Special Agent's interaction with that architecture on national security-counterterrorism matters.**
1. Terrorism, as a national security threat, is beyond the scope of any single U.S. Government agency to effectively respond and mitigate the threat. As a result, counterterrorism is an enterprise effort, requiring cooperation and coordination across a host of U.S. Government agencies.
    - a. Central Intelligence Agency (CIA) – As America's principal human intelligence (HUMINT) agency, the CIA dedicates significant resources to recruiting and running foreign sources to gain insight into the plans, intentions, and capabilities of foreign terrorist threats. The CIA primarily operates overseas; however, through their National Resources Division, they maintain offices in the United States primarily for liaison purposes.



HSI maintains liaisons in various CIA divisions, including the Counterterrorism Mission Center (CTMC).

- b. National Security Agency (NSA) – As America's principal signals intelligence (SIGNINT) agency, the NSA has various Targeting Offices of Primary Interest (TOPIs) focused on terrorism threats.
  - c. Federal Bureau of Investigation (FBI) – the FBI is a hybrid law enforcement agency and domestic intelligence agency. Within the United States, the FBI has primary jurisdiction for all counterterrorism investigations. However, the FBI does not have sufficient resources to manage the issue alone, so therefore all counterterrorism investigations occur under the auspices of the Joint Terrorism Task Forces resident at each of the FBI's 56 field offices.
    - 1) HSI is the single largest contributor of personnel to JTTF outside of the FBI.
    - 2) In FY18, HSI was a contributor in 78% of the 167 terrorist disruptions affected by JTTF nationwide.
    - 3) Almost half of JTTF disruptions employ HSI authorities.
    - 4) The HSI Headquarters element that has oversight over HSI participation on the JTTF is co-located with the FBI Headquarters Counterterrorism Division (CTD).
  - d. U.S. Special Operations Command (USSOCOM) – a unified combatant command under the Department of Defense that has operational control over U.S. special operations forces from the various military services (U.S. Navy Special Warfare, U.S. Army Special Forces, U.S. Marine Raiders, U.S. Air Force Special Operations, and others).
    - 1) The principal counterterrorism action element for the U.S. Department of Defense
    - 2) Since 9/11, highly networked with U.S. law enforcement. Investigative leads can come from Sensitive Site Exploitation (SSE) conducted by SOCOM elements on objectives in conflict zones.
    - 3) HSI has several liaison officers at SOCOM and its subordinate elements.
  - e. National Counterterrorism Center (NCTC) – NCTC, under the Office of Director of National Intelligence, is responsible for the integration and analysis of all counterterrorism information. It is staffed by a significant number of detailees from FBI and CIA. HSI has liaisons there, as well.
2. Terrorism databases
- a. Terrorist Identities Datamart Environment (TIDE)



1) TIDE is the U.S. government's central repository for known or suspected international terrorists (KSTs), and it is maintained by NCTC.

2) (b)(7)(E)

3)

4)

5)

b. (b)(7)(E)

3. Terrorist Screening Center (TSC)

- a. TSC was created in 2003 as a result of the 9/11 Attacks.
- b. TSC is a Multi-Agency Center administered by the FBI (the executive agency).

1) Other participants include members of federal law enforcement and other IC components.



- 2) Some TSC deputy positions held by DHS leadership.
- c. TSC is the U.S. Government's Consolidated Counter-Terrorism Watch-Listing Component and it maintains the Terrorist Screening Database (TSDB).
- d. Terrorist Screening Database (TSDB)

1) The TSDB is euphemistically known as "The Watchlist."

(b)(7)(E)

3) Subset of the TSDB

(b)(7)(E)

e. Handling Codes

1)

(b)(7)(E)

2)

3)



(b)(7)(E)

f.

(b)(7)(E)

Records

1)

(b)(7)(E)

4. National Targeting Center (NTC)

a. Tracks potential TIDE hits traveling to or from the U.S.

b.

(b)(7)(E)

c.

(b)(7)(E)

**Notes:**



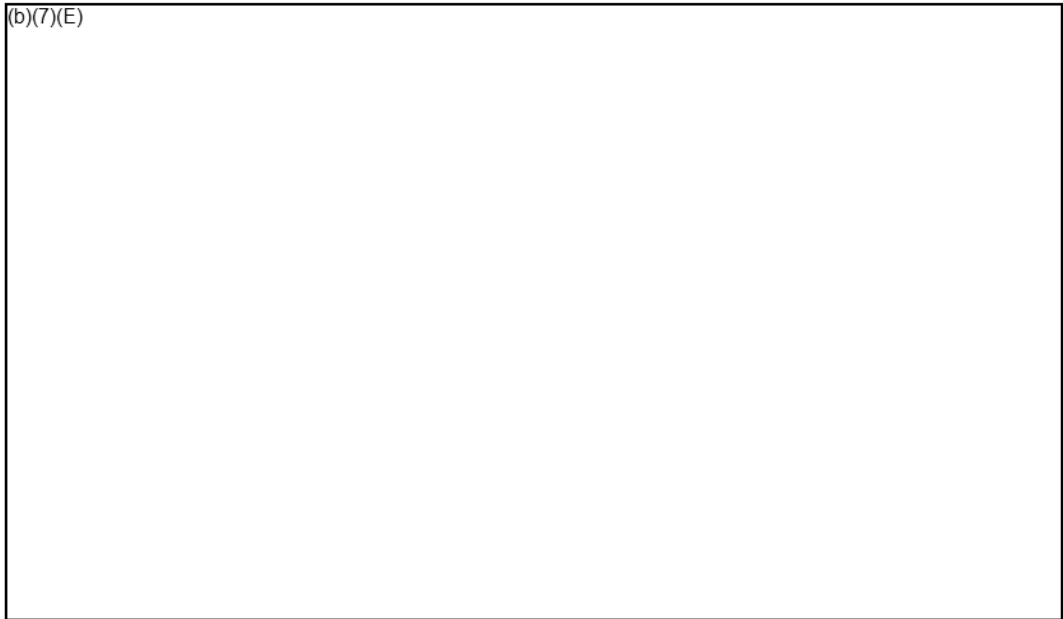


**H. EPO 8: Demonstrate knowledge of HSI's National Security Investigations Division (NSID) programmatic areas, NSID policies and procedures, as well as the characteristics of NSID investigations.**

1. Characteristics of National Security and Counterterrorism Investigations Prosecutions

a. National Security and Counterterrorism Investigations

(b)(7)(E)



2) Fundamental goal of any counterterrorism Investigations is to prevent an attack.

a) The number one priority is to neutralize a subject's ability to conduct a terrorist attack.



(1) Potential methods of neutralization

(b)(7)(E)

3) Two (2) aspects of national security and counterterrorism investigations that differ from other criminal investigations:

(b)(7)(E)

Page 2718

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

2. HSI Headquarters programmatic units and corresponding investigations

a. Counterterrorism Criminal Exploitation Unit (CTCEU)

1) CTCEU History

- a) Prior to the events of September 11, 2001, there was no effective system in place to accurately monitor the status of foreign students and other visitors in the U.S., with disastrous consequences.
- b) The Counterterrorism and Criminal Exploitation Unit within the National Security Investigations Unit (CTCEU) is responsible for combating security vulnerabilities that are criminal in nature or pose a potential threat to the U.S.

2) CTEU Mission: To prevent terrorists and other related criminals from exploiting the nation's immigration system and to expand the resource equities within the Intelligence Community (IC) and federal agencies.

a) This goal is accomplished by:

- (1) (b)(7)(E)
- (2)

Page 2720

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2721

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2722

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2723

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2724

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2725

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2726

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

6) Visa Life-Cycle Program

- a) Goal is to allow HSI to continuously monitor, vet, and identify any derogatory information on foreign visitors which may arise during the validity for their respective non-immigrant visa.

b) (b)(7)(E)

c)

3. Student Exchange Visitor Program (SEVP)

- a. SEVP Mission: To collect, maintain, and provide reliable information on foreign students and exchange visitors present in the U.S.
  - 1) Established to more effectively manage information on foreign students and exchange visitors in the U.S.
  - 2) Seeks to balance homeland security with the desire to continue to permit legitimate foreign students and exchange visitors to participate in high quality U.S. academic and exchange programs.
  - 3) Since September 11, 2001, SEVP's national security responsibility has been strengthened through collaboration with CTCEU, which focuses on preventing criminals and terrorists from exploiting the nation's immigration system through fraud.
  - 4) In order to sponsor foreign students and exchange visitors, institutions and programs need to apply and be certified by SEVP as an entity that can sponsor such individuals.
  - 5) SEVP is the HSI program that administers SEVIS and conducts outreach with the educational community.



- a) SEVP approves schools and programs for certification to enroll nonimmigrant foreign students and cultural exchange visitors and withdraws such certification when the school or program is determined to be no longer eligible.
- b) SEVP maintains information on schools/programs that apply for certification and those currently certified by SEVP:

Includes the Petition for Approval of School for Attendance by Nonimmigrant Student (Form I-17) and supporting documentation

- c) SEVP is able to audit records to ensure compliance by an institution or exchange program and can decertify an institution/program for non-compliance.
- d) SEVP has regional representatives who are responsible for liaising with institutions/programs in their geographic area.
- e) Regulations guiding the certification of schools and exchange visitor programs are located at 8 CFR §214 and 22 CFR §62.
- f) Once certified, Institutions and programs can sponsor students/visitors on:
  - (1) Nonimmigrant "F" Visas: Student in an Educational Program
  - (2) Nonimmigrant "M" Visas: Student in a Vocational Program
  - (3) Nonimmigrant "J" Visas: Cultural Exchange Visitors

b. SEVIS

- 1) The Student & Exchange Visitor Information System (SEVIS) is a web-based system that maintains accurate and current information on nonimmigrant students (F and M visa), exchange visitors (J visa), and their dependents (F-2, M-2, and J-2).
  - a) SEVIS enables schools and program sponsors to transmit mandatory information and event notifications, via the Internet, to DHS and DOS throughout a student's or exchange visitor's stay in the U.S.
- 2) SEVP is the HSI program that administers SEVIS and conducts outreach with the educational community.
- 3) The information contained in SEVIS is entered by the various academic institutions and exchange visitor programs.
- 4) Immigration Status vs. Visa Status



- a) It is important to remember that a visa is merely an invitation to present oneself at a port of entry and apply with CBP for admission.
- b) If one is coming to the U.S. on an F/M/J visa, once admitted, the person is eligible to remain in the U.S. as a non-immigrant for the duration of their course of study or program participation (aka Duration of Status).
- c) The revocation of a non-immigrant's visa after they have been admitted and are present in the U.S. does not make that person removeable – because they have been admitted for the duration of their status.

A visa revocation would only prevent a non-immigrant from being re-admitted to the U.S. on that visa should they decide to leave – i.e. visa has been revoked and the individual no longer has the right to present themselves at a POE at apply for admission with CBP.

- c. Responsible Officers (ROs) are individuals designated by an exchange visitor program to perform duties pertaining to SEVIS.
  - 1) Though responsible for maintaining exchange visitor's records, these individuals are often not physically located where the exchange visitor is participating in his/her program.
- d. Designated School Official (DSOs) are individuals selected by an academic institution to perform duties pertaining to SEVIS.
  - 1) DSOs input all data in SEVIS and issue I-20s.
  - 2) These individuals do not undergo background checks and are not vetted by the government.

A sample Form I-20 is in the Trainee Guide.

- e. Certificate of Eligibility for Nonimmigrant Student Status (I-20s)
  - 1) I-20 Form is issued by an SEVP participating institution to a foreign national applying for enrollment in a program offered by that institution.
  - 2) Receipt of the I-20 enables the foreign national to apply for a non-immigrant visa at a U.S. Embassy or Consulate.
  - 3) Once received, the non-immigrant "F," "M," or "J" visa holder may travel to the U.S. and apply for admission with Customs and Border Protection at a POE.
  - 4) Once admitted, the "F," "M," or "J" visa holder can stay in the U.S. for the length of time required to complete their program or course of study.



f. Interplay with CTCEU

- 1) SEVP and CTCEU are closely aligned as a large majority of CTCEU targets are present in the U.S. as SEVP participants.
- 2) SEVIS Exploitation Section (SES)
  - a) Section within CTCEU that combats criminal and administrative violations of the SEVP
  - b) SEVP Analysis and Operations Center (SAOC)

(b)(7)(E)

- 3) The SES carries out its mission by:

(b)(7)(E)

- 4) Indicators of SEVP Institutional (School) Criminal Fraud

a)

b)

c)

d)

(b)(7)(E)



(b)(7)(E)

e)

f)

g)

h)

i)

j)

k)

l)

m)

n)

o)

p)

- 5) HSI SAC offices may request the withdrawal of a school's SEVP certification by contacting the CTCEU.
  - a) Request must be accompanied by supporting documentation outlining the justification for the withdrawal.
  - b) Final authority for the withdrawal of a school's certification rests with the SEVP School Certification Branch (SCB).
  
- 6) HSI SAC Offices may also request that specific DSO's SEVIS access be revoked by contacting CTCEU.





- a) Request similarly must be accompanied by supporting documents outlining the justification for the DSO's ineligibility.

7) Administrative Violations Relative to a Student Status Violator

a)

(b)(7)(E)

b)

g. Family Education Right to Privacy Act (FERPA) and SEVP

- 1) FERPA (20 U.S.C. §1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records.
- 2) FERPA applies to all schools that receive funds under an applicable program of the U.S. Department of Education.
- 3) DHS Authority to Collect Information Related to Educational Programs.

- a) DHS's authority for collecting information on SEVP students is contained in 8 U.S.C. §1101 and 1184.
- b) The Department of State and DHS use this information to determine the eligibility for the benefits requested.

4) Authorization to Release Information by School

- a) DHS requires SEVP participating schools to provide the name, country of birth, current address, immigration status, and certain other information on a regular basis or upon request.
- b) The student's signature on the Form I-20 (Certificate of Eligibility for Nonimmigrant Student Status) constitutes an authorization for release of the student's records to any official from DHS.



(b)(7)(E)

4. Human Rights Violator And War Crimes Unit (HRVWCU)
  - a. Mission
    - 1) HSI is the lead federal law enforcement agency charged with investigating Human Rights Violators and War Crimes.
    - 2) HRVWCU was created to place a greater emphasis on investigating, prosecuting, and removing individuals who committed acts of torture, genocide, extra judicial killings, or severe forms of religious persecution.
    - 3) Core Mission
      - a) Deny human rights violators safe haven in the U.S. of by utilizing all of HSI's investigative techniques and legal authorities to identify, locate, investigate, prosecute and remove human rights violators, and war criminals from the U.S.
      - b) Prevent entry to the U.S. of human rights violators and war criminals.
  - b. HRVWCU Responsibilities
    - 1) Identifying suspected human rights violators
    - 2) Generating investigative leads which are then forwarded to the respective HSI field office(s)
    - 3) Providing intelligence, research, and coordinating intra-agency / international investigations
    - 4) Programmatic oversight of all HSI investigations relating to individual human rights violators, war criminals, and/or individuals implicated in acts of torture, genocide, or war crimes
  - c. Human Rights Violator War Crimes Center (HRVWCC) and its Components
    - 1) HRVWCU is a component of the overarching Human Rights Violator War Crimes Center.
    - 2) HSI is the lead executive agency for the HRVWCC.
    - 3) Human Rights Law Section (HRLS), a section within ICE's Office of the Principal Legal Advisor (OPLA), similarly situated under the HRVWCC umbrella
      - a) HRVWCC HRLS Historians



- (1) HRVWCC can provide direct case support to ongoing criminal and administrative investigations via historians who are available to assist with necessary historical research.
- 4) The FBI's Genocide and War Crimes Unit (GWCU) also operates under the HRVWCC.
- 5) HRT3 (Human Rights Violators Targeting and Tracking Team):
  - a) Seeks to identify foreign human rights abusers/war crimes suspects, and to "target" them in such a manner that they can be identified and properly vetted regarding their admissibility under the INA.

(b)(7)(E)

d. Human Rights Violations and War Crimes

- 1) Substantive Charges are the initial focus of all HRVWC cases
- 2) Substantive HRVWV charges include:
  - a) 8 U.S.C. 1091 – Genocide
  - b) 18 U.S.C. 2340a – Torture
  - c) 18 U.S.C. 2441 – War Crimes
  - d) 18 U.S.C. 2442 – Recruitment of and/or Use of Child Soldiers
  - e) 18 U.S.C. 181 – Peonage
- 3) When possible, substantive charges can be used separately or in conjunction with the charges related to benefit fraud.
- 4) If substantive charges cannot be proved or where jurisdiction of these substantive offenses cannot or will not be exercised, HSI pursues criminal charges related to visa and benefit fraud.
  - a) 18 U.S.C. 1546 – Fraud and Misuse of Visa, Permits or other Documents
  - b) 18 U.S.C. 1425 – Unlawful Procurement of Citizenship or Naturalization
  - c) 18 U.S.C. 1001 – False Statements or Entries Generally



d) 18 U.S.C. 1621 – Perjury

(b)(7)(E)

e. Administrative enforcement, under INA

1) Participation in Nazi persecution

- a) § 212(a)(3)(E)(i)
- b) § 237(a)(4)(D)

2) Genocide

- a) § 212(a)(3)(E)(ii)
- b) § 237(a)(4)(D)

3) Torture

- a) § 212(a)(3)(E)(iii)(I)
- b) § 237(a)(4)(D)

4) Extrajudicial Killing

- a) § 212(a)(3)(E)(iii)(II)
- b) § 237(a)(4)(D)

5) Severe Violations of Religious Freedom

- a) § 212(a)(2)(G)
- b) § 237(a)(4)(E)

6) Recruitment or Use of Child Soldiers

- a) § 212(a)(3)(G)
- b) § 237(a)(4)(E)

f. HRVWC Investigations – Lead Development

- 1) Leads for HRVWC cases can come from a variety of sources.
- 2) These include:

Page 2736

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



## Demonstration

### Demonstration Scenario

(b)(7)(E)



## Trainee Practice

Review the scenario and answer the questions.

### Practice Scenario

(b)(7)(E)



## 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 CIP and in HSISAT.

## Advance Organizer of Main Ideas

This lesson focuses primarily on the various types of electronic surveillance equipment, specifically (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 (IRs), 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. (b)(7)(E)

**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) (b)(7)(E)
  - 2)
  - 3)
-



(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)(C) 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)
  - (b)(7)(E)
  - a. (b)(7)(E)
  - b. (b)(7)(E)

**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:**

[Empty box for notes]

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

(b)(7)(E)

[Large empty box for content]

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 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.

# **US Immigration and Customs Enforcement Homeland Security Investigations Training**

## **HSI Academy**



## **HSI Evidence Processing 211311**

### **Student Guide**

## **HSI Academy Courses**

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). This contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, to anyone outside the HSI Academy, or to other personnel who do not have a valid "need-to-know" without prior approval of the HSI Academy Chief or his designee.



## Evidence Processing

### Motivation

Evidence consists of drugs, currency, packaging, documents, fingerprints, recorded statements, etc., which may support or establish violations of law. Evidence is gathered during investigations through search warrants, consent searches, Grand Jury subpoenas, administrative summonses, Purchases of Evidence (POE), undercover meetings, surveillances, wiretaps, trash runs, and numerous other means that are limited only by federal and state laws, statutes, and codes, as well as individual resourcefulness.

Searches and seizures consistent with Fourth Amendment protections are complex subjects for SAs. HSI search and seizure methods conform to constitutional and statutory limitations involving border operations and operations conducted in the interior of the United States. Statutes, regulations, and case law, including Supreme Court decisions, do not address every factual scenario. SAs also know the prosecutorial policies in their particular districts.

SAs make many decisions concerning searches and seizures in the field and, frequently, cannot consult reference materials, policy documents, or seek legal advice from their local Office of the Chief Counsel (OCC) or the appropriate U.S. Attorney's Office (USAO). It is important to understand and apply the principles of search and seizure laws, policies, and procedures. SAs must also recognize that search and seizure law is intricate and continually evolving.

When executing warrants, (b)(7)(E)

(b)(7)(E)

### Objectives

#### Terminal Performance Objective (TPO)

**Conditions:** Given a search warrant execution scenario, a set of case-related facts, and the presence of potential evidence,

**Behavior:** collect and process evidence

**Criterion:** in accordance with the Homeland Security Investigations Evidence Handbook HSI HB 15-05 / November 9, 2015, and in a manner which qualifies that evidence to be admitted in future criminal justice proceedings under the Federal Rules of Evidence.

#### Enabling Performance Objectives (EPOs)

**EPO 1:** Discuss the main objective in processing evidence.

**EPO 2:** Provide an overview of terminology, seizure authority, forms used, and roles and responsibilities involved in the seizure process.

**EPO 3:** Explain the process for evidence recovery and seizure from the pre-search planning phase to the post-search activities.



- |               |   |
|---------------|---|
| <b>EPO 4:</b> | Discuss procedures for storing evidence.      |
| <b>EPO 5:</b> | Discuss procedures for disposing of evidence. |

## Review of the Past

In CITP you learned how to conduct and document searches. In this course so far, you have received an overview of the types of cases for which HSI is responsible:

You learned that evidence consists of drugs, currency, packaging, documents, fingerprints, recorded statements, etc. You learned that items or property are seized, collected and processed in support of, or to establish, violations of the law. You learned that evidence is gathered during investigations through authorized legal means, which is limited only by federal and state laws, statutes, and codes as well as individual resourcefulness. You also received basic legal knowledge about dealing with evidence, including the consequences of deviating from established policies and procedures.

You learned that evidence should be carefully identified, packaged, and labeled; the goal of chain-of-custody is to demonstrate to the court that the evidence presented is in the same condition as when it was first seized.

During the legal instruction blocks of HSISAT you are exposed to the vast array of HSI legal authorities including those related to seizure and forfeiture. You have also been exposed, at this point in your training regimen, to Rule 41 of the Federal Rules of Criminal Procedure governing the execution of search warrants and the seizure of evidence.

## Advance Organizer of Main Ideas

In this lesson you will learn how HSI collects and processes evidence. Each of the items covered will be reinforced in an Evidence Processing Lab. This lesson begins with an overview of terminology, authority, forms, and responsibilities; followed by preparing for and conducting a pre-search briefing, a walk-through and labeling of the search area, and other tasks and activities to complete for use later in the investigation and proceedings. The location, document and establishment of chain of custody will be examined as well as how to safely and properly conduct the search, secure the search area, and complete the post walk-through and all necessary documentation. Finally, the packaging and labeling of all seized evidence will be discussed, as well as the storing and disposing of the evidence.

## Agenda

In this lesson, the instructor will emphasize the main objective of evidence processing, discuss evidence admissibility under the federal rules of evidence, introduce different types of evidence, and discuss the methods and procedures for collecting, processing, preserving, storing, documenting and disposing of seized evidence in accordance with the Homeland Security Investigations Evidence Handbook HSI HB 15-05 / November 9, 2015. The instructor will explain the concepts and provide a demonstration. Students will have an opportunity to practice the concepts in the Evidence Processing lab scenarios.





## INSTRUCTION

### Explanation

#### A. EPO 1: Discuss the main objective in processing evidence.

The main objective of evidence processing is to identify and collect various papers, effects, and other items that are useful in establishing the elements of the criminal law violations an HSI Special Agent is investigating.

1. Ultimately evidence identification, collection, and processing is for providing the basis of a prosecution of an identified offender.
  - a. Prosecution and could be federal or state
2. Use of seized evidence in prosecution
  - a. Need to establish admissibility: established through the collection and documentation of facts and details that establish the evidentiary foundation for a particular item sufficient to convince an independent magistrate to allow it to be admitted for consideration of the guilt or innocence of the defendant
    - 1) Foundation
      - a) Provenance of evidence
        - (1) Establish the origin of the item of evidence
          - (a) Circumstances of the item's identification and discovery
          - (b) Where the item was located
          - (c) What condition the item was found in
          - (d) Who found the item
          - (e) Supported by law enforcement photographs and sketch
      - b) Authenticity
        - (1) Item of evidence is what is purported to be
        - (2) Supported by Chain of Custody and other facts establishing that the item being presented in a prosecution is the same item that was identified, collected, preserved, documented, and stored during the course of the investigation
    - c) Relevance
      - (1) Item of evidence is what is purported to be



- (2) Supported by evidence documentation / Reports of Investigation
- (3) Supported by additional evidentiary processing resources; i.e. HSI Forensic Laboratory, CBP Document Laboratory, or other scientific or technical processing expertise

2) A HSI Special Agent must be able to testify to foundational / authenticity questions

- a) Can only be done by the “Finder” – the actual LE personnel who first discovered the item of evidence during the course of their operational duties
- b) Must be able to “recognize” the item of evidence

(1) (b)(7)(E)  
(b)(7)(E) ?”

c) SA must be able to testify as to how he/she recognizes the item of evidence.

(b)(7)(E)

d) SA must be able to testify in detail as to where the item was located and in what condition.

(b)(7)(E)



(b)(7)(E)

- e) SA must be able to testify that the item as it is presented during the prosecution is “in substantially the same condition” it was when it was first discovered.
  - (1) Serves to complete the necessary evidentiary foundation and provides the requisite authenticity to have the item admitted into evidence.

**Notes:**

**B. EPO 2: Provide an overview of terminology, forms used in evidence processing, and roles and responsibilities involved in the HSI evidence recovery and seizure process.**

The terms reviewed are from the HSI Evidence Handbook HSI HB 15-05 / November 9, 2015.

The Evidence Handbook establishes policies and procedures for the reporting, recordation, custody, handling, transfer, and disposition of seized property and evidence by ICE HSI Special Agents, Seized Property Managers (SPMs), and Seized Property Specialists (SPSs), as appropriate.

1. Definitions
  - a. **Abandonment:** Refers to abandoned property to which the owner has voluntarily relinquished all rights, title, claim, and possession without the intention of reclaiming any future rights thereto, such as retaking possession, reasserting ownership, or resuming enjoyment of the property.



b. **Detention:** Delaying or withholding the release of property pending a review for admissibility or proper importation or exportation.

1) (b)(7)(E)

c. **Fines, Penalties, and Forfeitures (FP&F) Case Number:** The (b)(7)(E) (b)(7)(E) and is used as the primary means for tracking seized and forfeited property and processing seizure cases. This number includes (b)(7)(E) (b)(7)(E)

d. **Forfeitable Evidence:** Evidence is seized property that is subject to forfeiture and is needed as evidence of the violation; it is the government's intent to keep this property from being returned to the listed owner when it is no longer needed as evidence.

**Note:** "The SEACATS code for Forfeitable Evidence is (b)(7)(E)"

e. **Forfeiture:** The legal process by which the ownership of property, such as real property, conveyances, aircraft, merchandise (including monetary instruments), bank accounts, etc., is transferred from its owner to the U.S. Government.

f. **Government-Generated Evidence:** Government-generated evidence is comprised of any evidentiary materials that are generated or obtained through various investigative means. Evidentiary materials include, but are not limited to, (b)(7)(E)

(b)(7)(E)

g. **High-Risk Evidence:** High-risk evidence is controlled substances, weapons and ammunition, and monetary instruments.

**Note:** The SEACATS SAS report code for seized property within this category is (b)(7)(E) or (b)(7)(E) (b)(7)(E)

h. **Incident Number:** The incident number is (b)(7)(E) (b)(7)(E) for tracking and identifying the type of enforcement action taken. This number includes (b)(7)(E)

(b)(7)(E)



(b)(7)(E)

- i. **Non-Forfeitable Evidence:** Seized property that is not subject to forfeiture, but is needed as evidence of the violation (e.g., documents, records, personal effects, and other property of value). This property was historically referred to as single-status evidence.

**Note:** The SEACATS code for Non-Forfeitable Evidence is (b)(7)(E)

- j. **Purchase of Evidence (POE):** The purchase of tangible items, including narcotics, with government funds during the course of an investigation. These items may be unlawful to own (e.g., counterfeit trademarked goods) or lawful (e.g., weapons, computers, or a sculpture purchased for the purpose of obtaining the fingerprints of the seller). Evidence that is purchased by SAs in furtherance of an investigation does not need to be forfeited, as the government already has title to the property by virtue of the purchase. As such, it becomes the property of HSI.

**Note:** Schedule I and II narcotics acquired through POE are classified as high-risk property, and must be documented on a SEACATS SAS report and turned over to the CBP SPS within established timelines.

- k. **Real Property:** Land and anything growing on, attached to, or erected on it, but excluding anything that may be severed without damage to the land.

**Note:** Real property is not considered "seized" until a Final Order of Forfeiture is received.

- l. **Search, Arrest, and Seizure Report (SEACATS SAS):** Used to record statistical and enforcement information relating to searches, arrests, and seizures made by HSI SAs and CBP Officers.

- m. **Seized Asset and Case Tracking System (SEACATS):** The official system of records for tracking seized and forfeited property from case initiation to final resolution.

1) SEACATS must be employed to record all seizures and forfeitures generated by HSI and CBP.

2) SEACATS produces (b)(7)(E)

- n. **Seizure:** The act of taking possession of any property by legal right or process. Seized property that is alleged to have been used in connection with or acquired through illegal activities may be subject to civil or criminal forfeiture. Property may also be seized to satisfy an unpaid judicial judgment, as long as proper notice of the amount due has been served.

- o. **ICM:** System ICM is an Integrated Case Management system. It is used to track information on suspect individuals, businesses, vehicles, aircraft,



and vessels. ICM can be used to access t (b)(7)(E)  
(b)(7)(E)

**Note:** ICM has replaced TECS.

**Notes:**

2. Evidence Seizure and Disposition Guides
  - a. Rule 41 of Federal Rules of Criminal Procedures
  - b. Homeland Security Investigations Evidence Handbook HD 15-05, November 9, 2015
  - c. Seized Asset Management and Enforcement Procedures Handbook (SAMEPH, July 2011)
  - d. 41 C.F.R. § 101-42.1102.10, "Firearms"
  - e. 41 C.F.R. Part 101-48, "Utilization, Donation, or Disposal of Abandoned and Forfeited Personal Property"
  - f. 41 C.F.R. Part 102-36, "Disposition of Excess Personal Property"
3. Chain of Custody Forms
  - a. **DHS Forms 6051:** Used to document the seizure of evidence and the chain of custody, as well as the transfer of custody of seized property/evidence.
  - b. There are five types of DHS Forms 6051 and they all contain instructions on how to complete them.
    - 1) **6051S**, "Custody Receipt for Seized Property/Evidence," is used to document property seized for a violation of law, evidentiary use in a criminal investigation, and transfers of custody
    - 2) **6051A**, "Custody Receipt for Detained or Seized Property/Evidence," is a continuation sheet and used as an



attachment for additional seized items, detentions, and/or additional signatures.

- a) DHS Form 6051A must accompany and/or be attached to DHS Form 6051S or DHS Form 6051D.
- 3) **6051R**, "Receipt for Property," is used to document and track the return of property that *is not* identified on the SEACATS SAS report (e.g., non-evidentiary items or personal effects).
- 4) **6051WT** and its attachment ensure that weapons are clearly identified by the FP&F case number, line number, description, and DHS Form 6051S.

**Note:** The seizure of weapons is more commonly documented in HSI investigations on Form 6051S.

- 5) **6051D**, "Detention Notice and Custody Receipt for Detained Property," is used to document property pending a review for admissibility or property importation or exportation.

4. Roles and Responsibilities

a. **Seized Property Manager (SPM):** Accountable for the security, handling, and inventory of seized and forfeited property. Responsibility extends to high-risk and forfeitable property held on a temporary basis and stored in any HSI field office. SPMs ensure that:

- 1) HSI personnel acting as SPSs/Evidence Custodians are performing their functions properly.
- 2) Physical security requirements are met for all seizures stored in field offices.
- 3) Proper justification exists for any high-risk and forfeitable seized property held by HSI.

**Note:** All high-risk and all forfeitable seized property will be held by HSI only on a temporary basis and for a defined purpose.

- 4) SEACATS records are properly updated in a timely fashion. Particular attention will be paid to ensure that the (b)(7)(E) code is up to date and that the property is correctly identified. Three types of legal status are used to identify property in SEACATS:

- a) (b)(7)(E)
- b)
- c)



- b. **HSI Seized Property Specialist (SPS):** Report directly to the SPM and ensure the preservation, safeguarding, and disposition of all seized property/evidence released to their custody. HSI SPSs coordinate pre-seizure analysis with the seizing officer, FPFO, CBP SPS, and the real property contractor. HSI SPSs also conduct and review SEACATS SAS reports to identify and account for seizure cases initiated (and canceled) within the SAC's AOR. They also:
  - 1) Assist the seizing officer, local CBP FP&F and SPS, and national property contractors, and provide assistance with pre-seizure analysis, when applicable.
  - 2) Ensure that the "Custody Receipt for Seized Property and Evidence" (DHS Form 6051S) (and "Custody Receipt for Seized Property and Evidence – Continuation Sheet" (DHS Form 6051A), if needed) is accurate and complete, and that the information mirrors the information on the SEACATS SAS reports and property inventory (i.e., verifying the FP&F/HSI case numbers, line item(s), quantities, descriptions, etc.), and immediately report any discrepancies to the SPM and the local FP&F field office.
  - 3) Ensure that SEACATS is updated within three (3) calendar days of a seizure, accept the property in SEACATS, and verify and update the (b)(7)(E) (b)(7)(E) codes.
- c. **Evidence Custodians:** SAs who are designated as the primary or secondary individuals responsible for the management of seized property/evidence rooms, and perform the same functions as the HSI SPSs.
- d. **Seizing Special Agents:** Ensure the timely and accurate completion of the SEACATS SAS report and case initiator forms (i.e., DHS Form(s) 6051; "Report of Drug Property Collected, Purchased, or Seized" (Drug Enforcement Administration (DEA) Form 7); etc.) for all property/evidence seized or otherwise obtained in enforcement activities.

**Note:** This can be the Case Agent, Evidence Custodian, or their designee on scene.

- e. **Case Agents:**
  - 1) Ensure the accurate inventory, security, storage, and disposition of all seized property/evidence generated throughout the investigation.
  - 2) Ensure that all seized property/evidence is disposed of prior to the closure of the investigative case record and file.
  - 3) Ensure timely input of complete and accurate data into SEACATS.





- 4) Ensure the completion and accuracy of the appropriate DHS Form(s) 6051.
- 5) Transfer seized property/evidence to permanent storage on a timely basis.
- 6) Forward cases and proper documentation to the FPFO on a timely basis.

**Notes:**

**C. EPO 3: Explain the process for evidence recovery and seizure from the pre-search planning phase to the post-search activities.**

1. Preparation

a.

(b)(7)(E)

2. Identify items which may be recovered/seized as evidence

(b)(7)(E)

3. Evidence recovery/seizure tools

(b)(7)(E)

Page 2202

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2203

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

**Notes:**

f. Laboratory Resources

- 1)
- 2)
- 3)

(b)(7)(E)

Page 2205

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

g. Identification of Evidence

- 1) Evidence must be carefully identified, packaged, and labeled without commingling or contaminating it with other seizures.



- a) Seized items must be within the scope of the Search Warrant.
- b) Articulate as being covered under Attachment B of the Search Warrant

**Notes:**

[Redacted Notes Area]

(b)(7)(E)

[Redacted Content Area]

Page 2208

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2209

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2210

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



## DEMONSTRATION 1 – PART 1

**Demonstration 1:** The instructor will demonstrate the use of evidence packaging and bagging supplies and show examples of the forms used during searches and seizures of evidence.

(b)(7)(E)

## STUDENT PRACTICE – CLASS EXERCISE

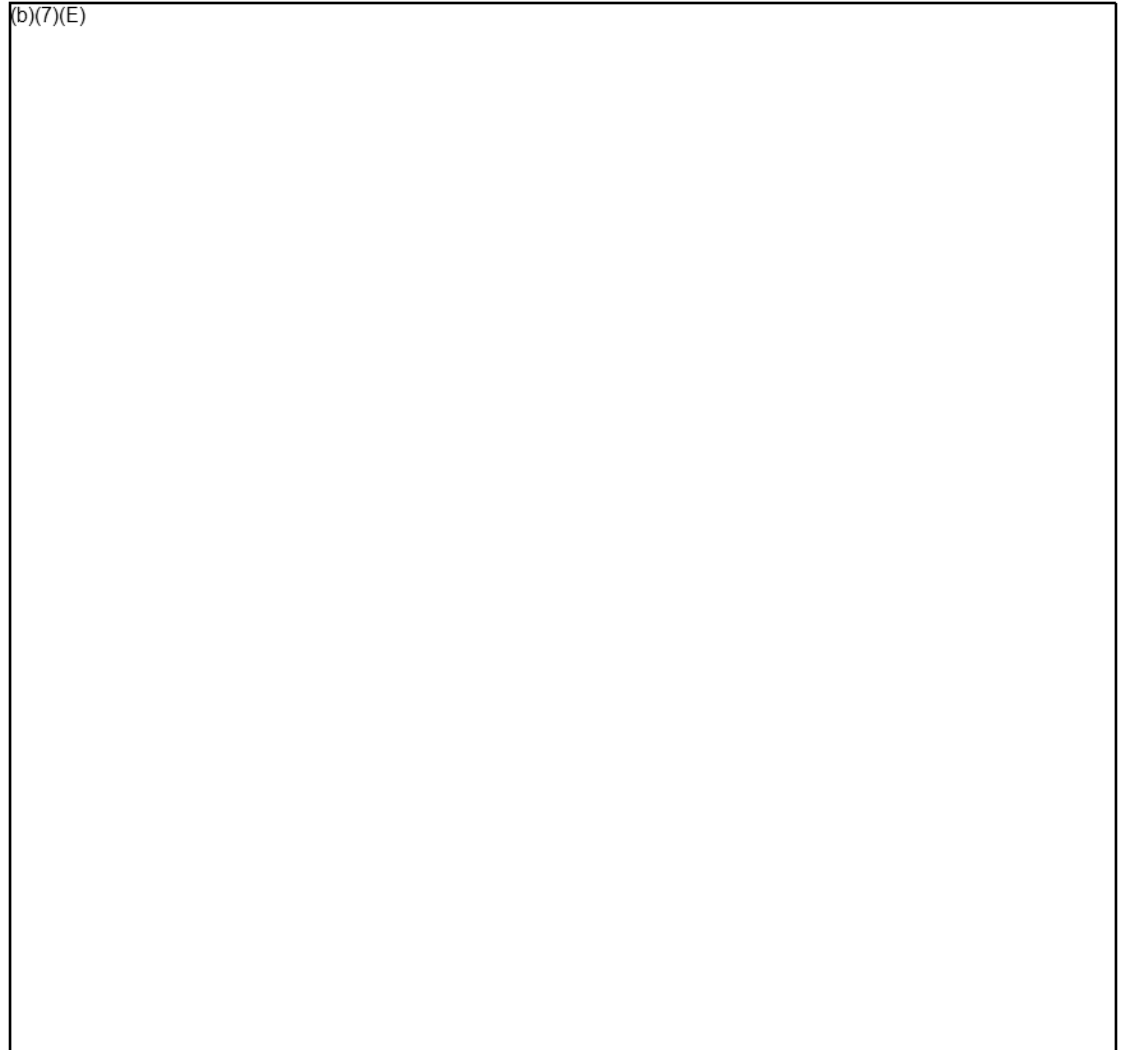
**Student Practice – Class Exercise:** You should be given an index card, an evidence bag, and a 6051S (or copy thereof). You should process the items of evidence in accordance with the (b)(7)(E) discussed above and exhibited via the demonstration.

### h. Types of Evidence

(b)(7)(E)



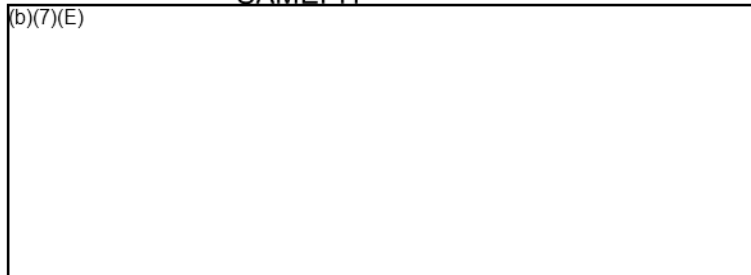
(b)(7)(E)



(2) Must be entered into SEACATS

- (a) The return of seized documents will be recorded on DHS Form 6051S (and DHS Form 6051A, if needed).
- (b) Upon completion of all judicial proceedings, the seized items will be disposed of in accordance with Section 11.9.14 of the SAMEPH

(b)(7)(E)





(b)(7)(E)

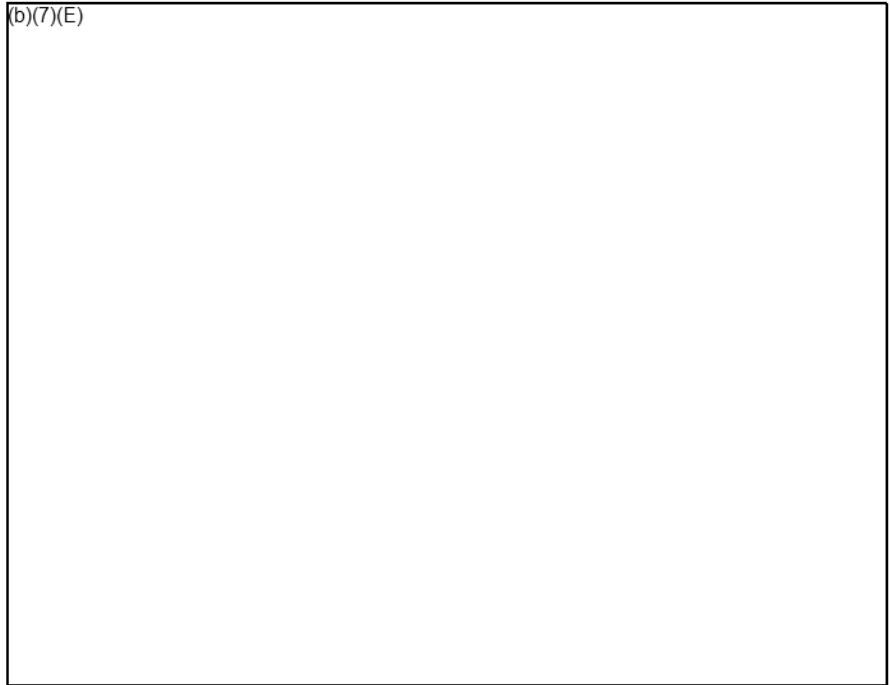
**Notes:**

- 2) Controlled Substances (High Risk)
  - a) Handling of controlled substances as evidence is covered in the Seized Asset Management and Enforcement Procedures Handbook (SAMEPH).
    - (1) Chapter 11 – ICE Related Seizures
    - (2) Chapter 11.9.6 – Controlled Substances
  - b) SAs should take the following into consideration:

(b)(7)(E)



(b)(7)(E)



(3) Damaged Containers:

(b)(7)(E)



(4)

(b)(7)(E)





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

c) Threshold amounts, representative samples, and retention

(1) 28 CFR 50.21

- (a) Heroin
- (b) Cocaine
- (c) Marijuana

(2) SAMEPH / Policy

(a) Controlled substances (not bulk marijuana)

- i. Policy: Controlled Substances (Non-Marijuana) can be submitted to laboratory in any quantity.
- ii. Thresholds to be retained will be IAW 28 CFR 50.21 and SAMEPH Sec. 11.9.6 and 4.1.18

(b) Bulk marijuana

- i. There are no threshold amounts defined for marijuana in 28 CFR 50,21
- ii. 1 KG "Representative Sample"
- iii. Representative Sample / Exemplar will be used for Testing
- iv. 10 separate 5-gram aggregate samples used for testing and taken from different, random locations within marijuana bulk (should document locations where samples are taken from; i.e. with photograph)



- v. SAMEPH 11.9.6 (that section references 4.1.18)

**Notes:**

d) Testing

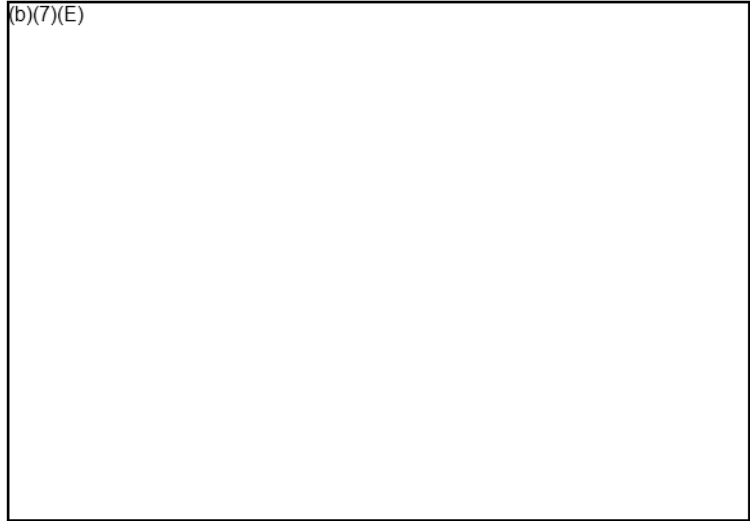
- (1) DEA Laboratory submissions for controlled substances (non-marijuana)

(b)(7)(E)





(b)(7)(E)



- (a) DEA Form 7: A written request for drug analysis to a DEA laboratory and the document upon which the laboratory results are recorded. It also serves as a receipt for the transmission of drug evidence to the laboratory for chain of custody purposes (the only instance when DHS Form 6051S is not used).

i.

(b)(7)(E)



ii.

- (b) In the event that there are multiple seizures of different types of controlled substances, each new type will receive a different exhibit number when recording the exhibits on DEA Form 7. For instance, a seizure of cocaine and marijuana would result in Exhibit 1, cocaine, and Exhibit 2, marijuana.

- i. Upon completing the drug analysis, DEA will furnish a report to the submitting HSI office. The return of the drug evidence to HSI will be documented on a "Receipt for Cash or Other Items" (DEA Form 12). A



copy of DEA Form 12 and a copy of  
DEA Form 7 will be attached to DHS  
Form 6051S (and DHS Form 6051A,  
if needed).

ii.

(b)(7)(E)

(c) Reality

(b)(7)(E)

(3) Testing and DEA Laboratory submissions for bulk  
marijuana

- (a) Marijuana evidence is often seized in quantities too large to be collected, handled, and disposed of in the same manner as other controlled substances.
- (b) The procedures for sampling bulk marijuana are as follows:

(b)(7)(E)



(b)(7)(E)

**Note:**

(b)(7)(E)

(b)(7)(E)

(4)

(b)(7)(E)

**Note:**

(b)(7)(E)

(b)(7)(E)

(5)

(b)(7)(E)

(6)

(7)

e)

Samples may be provided only to the defense counsel pursuant to a court order, a copy of which must be obtained by the case agent. The defense counsel will acknowledge receipt of any samples by signing the DHS Form 6051S (and DHS Form 6051A, if needed). Samples



will be in the smallest amounts agreed upon by the AUSA and defense counsel. Any independent laboratory that conducts testing for the defense counsel must be licensed by the DEA.

**Note:** See Section 4.1.18, "Pretrial Destruction of Bulk Drug Evidence," and Section 11.9.6. "Controlled Substances." Of the SAMEPH for specific information about the handling of bulk marijuana evidence.

**Notes:**

(1) Sealing and Packaging:

(b)(7)(E)

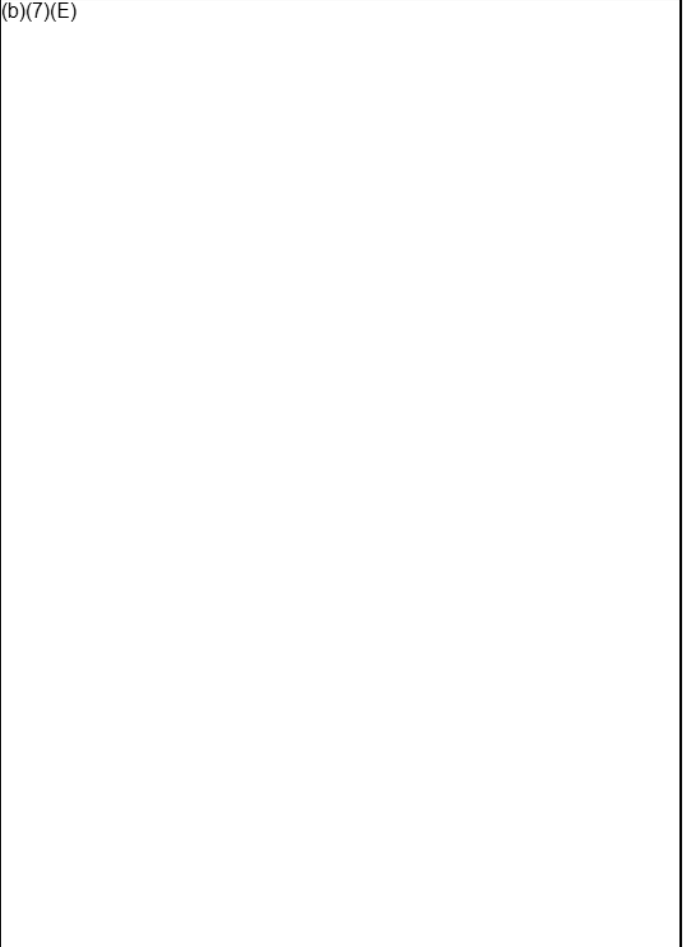
(2) Open and Resealing:



- (a) Under normal circumstances, evidence should be sealed once and submitted to the DEA laboratory. However, when the sealed evidence must be opened, it should be done without destroying the original seal. Upon resealing, the evidence and all parts of the old evidence bag or box should be placed in the new evidence bag, box, or package, and then resealed.

- i.  (b)(7)(E)
- ii.

(3) Mailing and/or Transporting:

- (a)  (b)(7)(E)
- (b)



(b)(7)(E)

iii

iv

v.

**Notes:**

3) Monetary and Negotiable Instruments (High-Risk)

a) Monetary and Negotiable Instruments

- (1) Monetary instruments, as defined in 31 C.F.R. § 103.11(u), include U.S. and foreign currency, traveler's checks, bearer negotiable instruments, bearer investment securities, bearer securities, stock on which the title is passed on delivery, and similar material.



- (2) Negotiable instruments include personal checks, business checks, cashier's checks, third-party checks, promissory notes, and money orders.
- (3) Money is the ONLY "fungible" evidence.

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

(b)

b) Collection and Processing

- (1) The seizing officer is responsible for the security of the seized currency and monetary instruments from the time of seizure until transfer to the CBP SPS. SAs are authorized to have temporary custody of seized currency or monetary instruments for examination or for presentation for criminal proceedings with approval from AFU.
- (2) The procedure for handling monetary instruments (excluding currency) is as follows:

(b)(7)(E)

- (3) The procedure for handling currency is as follows:

(b)(7)(E)



- (4) Conduct the inventory immediately, or as soon as reasonably practical, after seizure (responsibility of the seizing officer's supervisor).

(5) Sealing

- (a) (b)(7)(E)
- (b)

**Notes:**

c) Large Currency Seizures:

- (1) Seized currency collections arrangement for large currency seizures (b)(7)(E) (SAMEPH §4.3.11)

- (a) (b)(7)(E)
- (b)
- (c)





(d) (b)(7)(E)

(e)

(f)

(g)

**Notes:**

- 4) Weapons and Ammunition (High-Risk)
  - a) Firearms and ammunition should not be considered “contraband.”
    - (1) Can be seized as evidence / fruits / instrumentalities
  - b) SAs can only forfeit firearms and ammunition if the firearms and ammunition are:
    - (1) Used in a violation of federal law (e.g., smuggling, export violations)



- (2) Used in the commission of a crime
- (3) Purchased with criminally derived funds or proceeds
- c) (b)(7)(E) trace for weapons discovered and suspected of being used in criminal law violations but whose ownership / provenance is unknown.
- d) 18 USC §922(g) (5 – possession of a firearm by an alien
- e) Within 30 days of the date of seizure, SAs must notify the FPFO in writing of the intention to administratively forfeit the seized firearm and/or ammunition. SAs should consider forfeiture and grounds at time of seizure.
- (1) The notification may be made by (b)(7)(E)  
(b)(7)(E)
- f) **The method of last resort in disposing of firearms/ammunition is abandonment.** SAs will utilize DHS Form 4607 to document an owner's desire to abandon firearms and ammunition.
- g) **Firearms encountered during enforcement actions should be checked** (b)(7)(E)
- h) Weapons seized from individuals who do not legally own them must be stored as non-forfeitable evidence until federal or state prosecution is determined.
- i) Weapons that will not be forfeited and are no longer needed as evidence in a legal proceeding will be returned to their legal owner; their return must be documented on a DHS Form 6051S with a 6051R (Property Receipt).

**Note:** See Section 4.4.2 of the SAMEPH for further details on forfeiture authority and procedures.

**Notes:**

5) Fingerprints and Latent (Print) Evidence



a) Fingerprints

(1)

(b)(7)(E)

(2)

(3)

b) **Latent:** Evidence which is not visible to the naked eye

(1) **Latent print evidence**, to include fingerprints, can be found on almost an item depending on several factors including the item's surface texture

(2) Can use certain techniques to detect latency (i.e. oblique lighting with flashlight)

(3) If latent evidence discovered or suspected –

(b)(7)(E)

c) Apply same rules to all visible and latent print evidence (i.e. non-impression shoe prints)

6) Biological and Trace Evidence

a) Anticipated that based on HSI investigative disciplines that SAs will encounter new types of evidence

b) Biological and trace evidence requires specialized training to examine and store.

c) If anticipated/encountered, HSI SAs should partner with other federal, state, and local agencies who can assist in



the identification, collection, and storage of Bio/Trace evidence.

**Note:** HSI policy is specific to biological evidence but is silent regarding trace evidence. Because the same principles regarding identification, collection, and storage apply to trace evidence it would appear policy dictates that HSI Special Agents similarly partner with other properly trained and equipped agencies when it comes to trace evidence.

Purpose of partnering with other agencies is to ensure proper collection and preservation of evidence for use as evidence in a prosecution.

- d) Once collected, Bio/Trace evidence must be turned over to another qualified agency for preservation and storage.
- (1) Arrangements should be made for quick transfer to a local/state/federal crime lab for testing (i.e. serology/DNA testing).
  - (2) Policy prohibits seizure of Biological evidence by HSI Special Agents.

**Note:** Policy also prohibits collection by HSI SAs – does not prohibit HSI SAs from assisting personnel from another other qualified law enforcement agency recovering Biological evidence; there is no prohibition with respect to trace evidence)

- (3) Policy prohibits storage of Biological evidence (DNA/Bodily Fluids) in HSI seized property /evidence room or CBP permanent vault.
- (4) Policy references SAMEPH §5.4.6

Section Reads as follows:  
5.4.6 Blood-borne Pathogens

Any items that may contain blood-borne pathogens or bioterrorism agents (e.g., body fluids or parts, brain matter) will not be collected, seized by any case agent, or stored in any temporary or permanent seizure vault. When these items are encountered, the case agent should call a local or State agency with a lab that is equipped to deal with these materials. The local office should be familiar with lab facilities in its area and what they are equipped to handle. The case agent should



receive a lab report for court purposes, but the items will remain in the custody of the lab facility and are not entered into SEACATS.

- (5) Notably, there is no such restriction for other forms of “forensic” evidence i.e. latent, impression, tool marking, ballistic etc. evidence.

- (a) Best Practice (b)(7)(E)  
(b)(7)(E)

**Notes:**

7) Electronic Devices and Digital Media

- a) Rule 41 of the Federal Rules of Criminal Procedure authorizes the seizure of computer hardware that is evidence, an instrumentality, contraband, or the fruit of a crime.

- (1) In this instance, the seizing officer is completely justified in seizing the computer hardware and software and searching it off site.
- (2) In cases where hardware is a storage device for evidence of a crime, Rule 41(b) authorizes the issuance of a seizure warrant to search for and seize the digital evidence contained in the computer.

- (a) Rule 41(e)(2)(B) allows for a general procedure to seize digital and electronic storage media, remove it from the scene, and process at another location to facilitate review of the electronic contents contained therein.



- (b) This facilitates a thorough search for the digital evidence in a controlled environment.
- (3) Common Practice in Most Districts for Rule 41 Warrants are Attachments Cs.
  - (a) Dictate how long the USG has to process the actual seized digital and electronic storage media.
  - (b) Dictate how long the USG has to review the electronic information recovered from the seized digital and electronic storage media.
  - (c) Return the actual digital and electronic storage media if there is no contraband or other facts suggesting that the physical media itself is evidence/fruit/instrumentality.
  - (d) Review the processed electronic data from the devices. If evidence is found, the HSI Special Agent will seize the forensic image and document on a 6051S (will be considered Government Generated Evidence, stored as such, and not inputted into SEACATS.

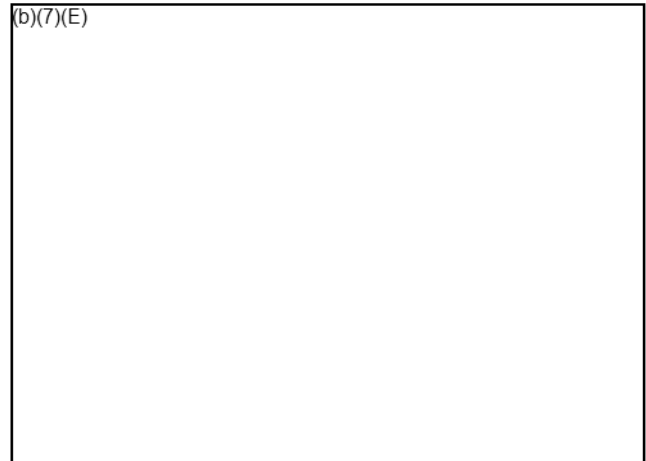
(4) Basic Rules for handling DSM/ESM as evidence:

- (a) (b)(7)(E)
- (b)
- (c)
- (d)
- (e)
- (f)



(g)

(b)(7)(E)



- b) It is strongly recommended that, before seizing any electronic device or digital media, the seizing officer consult with an HSI Computer Forensic Agent. The seizing officer should refrain from removing components from computer systems. Removal of the components may impede or prevent the recovery of valuable digital evidence contained within the storage devices.

**Notes:**



i. Special Classifications of Property and Evidence

1) Purchased Evidence (POE)

- a) Evidence that has been purchased by the U.S. Government in furtherance of an investigation does not need to be forfeited. This is because title to the purchased evidence transfers to the U.S. Government with payment.
- b) The person or entity from whom the evidence was acquired no longer has any standing with regard to title or ownership; therefore, it is not subject to seizure or forfeiture and need not be entered into SEACATS.
- c) Controlled Substances: Schedule I and II controlled substances are the only POE items that must be entered into SEACATS upon purchase. These items are to be



turned over to the CBP SPS for secure storage and final disposition.

- (1) (b)(7)(E)
- (2)

d) Firearms: Within 72 hours of the purchase of a firearm, suppressor, destruction device, electrical muscular disruption device, or other lethal weapon, the Responsible Official, as defined by the Interim ICE Use of Force Policy, dated July 7, 2004, or as updated or superseded, must submit a memorandum to the Assistant Director, Office of Firearms and Tactical Programs (OFTP), certifying the acquisition and possession of the item(s).

- (1) The memorandum must include the following information:

- (a) (b)(7)(E)
- (b)
- (c)
- (d)
- (e)
- (f)

- (2) Within 72 hours of the purchase, the firearms must be shipped to (b)(7)(E) (b)(7)(E) (b)(7)(E) (b)(7)(E) unless there is an immediate investigative or evidentiary need.

- (a) (b)(7)(E)
- (b)





(b)(7)(E)

2) Government-Generated Evidence

a) Includes, but is not limited to, trash or items obtained from garbage made available for pick-up, records received from the service of administrative subpoenas and summonses, electronic evidence "carved out" from a seized computer or other electronic devices, mirrored hard drives and/or computer-related media, surveillance photographs, consensually monitored electronic recordings, emails or electronic data received from Internet Service Providers (ISPs), or other third parties acquired through a federal search warrant or other legal process, POEs (except schedule I and II controlled substances), etc.

- (1) This type of evidence should not be entered on a SEACATS SAS report for accountability purposes.
- (2) Includes evidence obtained pursuant to Electronic Communications Privacy Act (ECPA) search warrants and orders
- (2) Evidentiary material(s) of this type must be recorded on DHS Form 6051S (and DHS Form 6051A, if needed), and stored in the HSI seized property/evidence room.
- (3) These items must be segregated from the storage of seized property.
- (4) The SAC has the discretion of allowing storage of electronic surveillance evidence to be maintained by the designate Technical Enforcement Officer.
- (5) SAs will document electronic evidence obtained from ISPs or forensic images of electronic media subsequent to a search warrant using an ROI type code "6" (Search Warrant executed on ISP/Digital/Electronic Media).

b) Evidence gathered during an investigation may be electronic surveillance evidence obtained from officers, witnesses, or suspects through consensual and non-consensual recordings.

- (1) An identification label including (b)(7)(E)  
(b)(7)(E)
- (2) General rules regarding evidence collection, packaging, documenting, preservation, chain of



custody and storage should be applied to Government Generated Evidence

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

(3) Best Evidence Rule

- (a) Original electronic media such as compact disks (CDs), flash drives, digital recorders, smartphones, tablets, and computers should not be erased, recorded over, or discarded.
- (b) Original notes, media, and transcripts (regardless of form) must be preserved for possible presentation in court. Original recorded media must be documented on DHS Form 6051S (and DHS Form 6051A, if needed) for tracking and secure storage.

- i. Original notes should be preserved (b)(7)(E) by the case agent.
- ii. Participating Agents' original notes (b)(7)(E) safekeeping but PAs should keep a copy of their notes from reference purposes.
- iii. Original notes should not be placed into evidence.
- iv. Transcripts should be considered as notes for this purpose and should similarly be preserved as part of the (b)(7)(E)

(4) Malfunctioning media devices must not be discarded. The media should be saved and marked

(b)(7)(E)

(b)(7)(E)

(5) Original recordings should be stored with the

(b)(7)(E)

3) Personal Property

- a) Personal effects or items that cannot be described as either fruits or evidence of the crime.



- (1) Discovery of currency on a person or in his or her conveyance at the time of the arrest and/or seizure does not automatically make it subject to seizure and forfeiture, unless circumstantial evidence of proceeds of a crime exist to support the seizure and there is an appropriate forfeiture statute enforced by HSI.
- (2) Other personal effects such as watches, wallets, costume jewelry, and other miscellaneous items bearing no nexus to criminal activity or proceeds of a crime may not be indiscriminately seized. Reasonable and prudent efforts should be taken at the earliest possible opportunity to transfer the personal effects to an authorized representative of the arrestee/detainee.

b) Guidelines:

- (1) At the time of seizure or arrest, a 100 percent inventory shall be taken of all personal effects of the arrested individual. An inventory must also be taken if the personal items are commingled with other seized evidence.
- (2) HSI supervisors will ensure, whenever it is safe and practical, that the seizing/arresting officer complete the personal effects inventory, with a second law enforcement officer present, in the presence of the violator.
- (3) In situations where officer safety is imperiled, a personal effects inventory in the presence of the violator may be waived; however, this action should be reported to the SA's first-line supervisor at the earliest possible time and documented in the case file.
- (4) A DHS Form 6051S (and DHS Form 6051A, if needed) must be used to document the inventory of the personal effects taken from the violator.
- (5) If the arrestee/violator is transferred to Enforcement and Removal Operations for removal proceedings, the personal effects/property will accompany the violator.
  - (a) If the violator voluntarily abandons the property, a "Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise" (DHS Form 4607) will be completed by the seizing/arresting officer, witnessed by another officer, and signed by the violator.



- (6) When personal effects are released to a violator, the violator's authorized agent, or any other agency, person, or entity, the individual who is receiving the personal effects must sign DHS Form 6051S (and DHS Form 6051A, if needed), showing acceptance of the items.
- (7) Abandoned and unclaimed seized items that are neither evidentiary nor needed as evidence must be disposed of in accordance with ICE Personal Property Operations Handbook, dated April 8, 2013, or as updated, and Section 11.9.14 of the SAMEPH.

**Notes:**

- 4) Abandoned Property
  - a) Abandoned property is property for which the owner has relinquished his ownership interest.
  - b) Actual Declared Abandonment
    - (1) Document on DHS Form 4607 – Notice of Abandonment and Assent to Forfeiture of Prohibited or Seized Merchandise
    - (2) Signed by the property's owner
      - (a) Can be the Violator but not always
    - (3) Abandoned Property Documented and seized on a 6051S
  - c) Constructive Abandonment
    - (1) Property located in a condition that suggests it has been abandoned (i.e. trash items)
    - (2) "Trash Run" Items – document on 6051S



- (a) Not entered into SEACATS
- (b) Considered by agency a form of government generated EVD
- (c) Stored like government generated EVD

**Notes:**

- j. Packaging and Sealing of Evidence
  - 1) General requirements
    - a) DO NOT comingle evidence

(b)(7)(E)

**Note:** Additional information on labeling requirements can be found in Section 2.8.16-17 of the SAMEPH.

- b) Sealing considerations



(b)(7)(E)

- (3) Unsealing evidence
- (a) If unsealing evidence bag, preserve original evidence bag and include in new evidence bag along with evidentiary items themselves.
- c) Multiple evidence containers
- (1) When more than one container is used to seal a single line item, the containers must be numbered (b)(7)(E) and a copy of the completed DHS Form 6051S (and DHS Form 6051A, if needed) must be placed on the first container only.
- d) Flammable, volatile, or potentially toxic evidence
- (1) Identify all dangerous evidence (flammable, volatile, or toxic) on the exterior of the evidence packaging.



(b)(7)(E)

- e) Evidence delivered or redelivered to the HSI/CBP SPS or appropriate national contractor must be properly sealed in approved evidence bags or boxes. Seizure bags that have been opened or damaged must be resealed in new seizure bags. SAs must maintain and place the old bag into the new bag for evidentiary and court purposes and annotate the new bag number on the DHS Form 6051S.

(1)

(b)(7)(E)

2) Types of acceptable evidence containers

(b)(7)(E)

k. Handling and documenting evidence

1) Use protection when collecting evidence

a) Gloves

(b)(7)(E)

b) Eye protection



- (1) Protection when dealing with controlled substances
    - c) Mask
      - (1) Protection when dealing with controlled substances especially highly toxic narcotics (i.e. Fentanyl)
    - d) Tyvek suit
      - (1) When needed to appropriately collect, handle, and preserve biological and trace evidence
  - 2) Mark evidence packaging or containers
  - 3) Different types of evidence can necessitate different containers
    - a) Porous vs. Non-porous
  - 4) Complete evidence log with appropriate notations for each item of evidence
  - 5) Avoid excessive handling of evidence after recovery
    - a) SAs should minimize the number of law enforcement officers having custody of the evidence
  - 6) Seal all evidence containers at the crime scene
    - a) Can be dependent based upon what the item is and review issues
  - 7) (b)(7)(E)
  - 8) Constantly check paperwork, packaging notations and other pertinent recordings of information for possible errors which may cause confusion or problems at a later time.
- I. Provide collected evidence to Evidence Custodian
- 1) Evidence Custodian manages seized property/evidence rooms.
  - 2) (b)(7)(E)
- m Prepare DHS Form 6051S (an DHS Form 6051A, if needed)
- 1) Discuss completing a 6051S
    - a) Focus on the entry of evidence in the line item area
      - (1) Packaging/Numbers/Type
      - (2) Can use more than one line for description





- (3) Description should match Finder's notation and evidence bag/container
- (4) Discuss when to assign the items

(b)(7)(E)

- (5) The line item numbers and property descriptions on the DHS Form(s) 6051 must accurately reflect the line numbers documented on the SEACATS SAS report.
- (6) Separate DHS Forms 6051S must be completed for property line items that have different category type codes and property type codes; for example:

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

(b)

(c)

(d)

- (7) Separate DHS Form 6051S must be utilized for all seized property items that will follow different custody routes and different storage locations.

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

(b)

- (8) Forfeitable and non-forfeitable evidence must be listed on separate DHS Forms 6051S.
- (9) Discuss "splitting" 6051s and how to do so.
  - (a) Required when custody route for a particular item of evidence diverges from other items originally listed on the same 6051. Need to track the divergent evidentiary item on a new 6051S, annotate new 6051 number in the chain of custody section of old 6051S, in the remarks section



of the new 6051S, and attach a copy of the new 6051S to the old 6051S.

- (10) Discuss use and importance of the "Remarks" Section of the 6051
- (11) Evidence Specific Issues

(b)(7)(E)

(a)

(b)

(c)

**Notes:**

b) Chain of Custody

- (1) The original DHS Form 6051S (and DHS Form 6051A, if needed) must remain with the evidence as the evidence moves from one person to another, into or out of the seized property/evidence room, etc. One copy will be maintained in (b)(7)(E)

(b)(7)(E)

- (2) Exception: The original DHS Form(s) 6051 must not remain with the evidence when "suspected controlled substances" are sent to the DEA laboratory for analysis, or to any other entity outside of HSI or CBP. DHS Form 6051S (and DHS Form 6051A, if needed) will again be used for



documenting the chain of custody when the narcotics are later retrieved from the DEA laboratory. DEA Form 7 is used to document the request for drug analysis and DEA laboratory results.

- (3) Original DHS Form 6051S must accompany the seized property/evidence to the specific storage location(s) or property custodian.
- (4) Every time property is released or transferred from one individual to another (upon every change in custody), the receiving officer must take custody of the property by signing the DHS Form 6051S (and DHS Form 6051A, if needed).
- (5) If the releasing officer is not the last individual to sign the chain of custody, he or she must sign the DHS Form 6051S (and DHS Form 6051A, if needed) prior to release and transfer to the person receiving the property.
- (6) 

(b)(7)(E)
- (7) When completing a DHS Form 6051S for evidentiary items such as government-generated evidence, 

(b)(7)(E)

 must not be included at the top of the form(s) because these items are not entered into SEACATS.
  - (a) There will not be incident or FP&F case numbers generated for these items.
  - (b) Annotate on all 6051s for government generated evidence, POE (non-controlled substances), and the like "NOT IN SEACATS."
- (8) Seizing SAs may use a separate original DHS Form 6051S for each line item so that the chain of custody for each item is easier to determine and more accessible.
  - (a) When using this method Special Agents need to ensure the same line item number for a specific event is not utilized more than once.
  - (b) DHS Form 6051S must be attached to each individual package using a sleeve or press-on envelope.
  - (c) SAs must not attach the DHS Form 6051 by taping, stapling, rubber bands, heat seals,



etc. (b)(7)(E)  
(b)(7)(E)

**Notes:**

4. Post-Search Activities and Wrapping Up Search Warrant
  - a. Recover and account for search equipment
  - b. Remove room labels
  - c. Leave copy of warrant and inventory
    - 1) Once completed, leave copy of warrant and inventory of seized property with the owner or occupier of the premises.
      - a) If no one is available to accept copies of search warrant and inventory/receipt of items taken, take a photograph of these items where they are left in the crime scene.
      - b) SAs do not need to show a copy of the warrant to the occupants of the premises prior to or during the execution of the search warrant.
      - c) If owner or occupier of premises is not present or is arrested during the execution of the search warrant, take steps to secure premises before leaving, especially if the execution of the warrant required a forced entry.
    - 2) Return the search warrant and inventory of seized property
      - a) Usually the issuing magistrate – warrant designates the specific judge or magistrate.
      - b) SAs should return the search warrant as soon as possible.
    - 3) Case agent or team leader documents the warrant in a detailed Report of Investigation (ROI).
    - 4) Evidence and contraband seized during the execution of the search warrant handled in accordance with the HSI HB 15-05 Evidence Handbook and HSI policies on evidence.
  - d. Account for all personnel



e. (b)(7)(E)  
f.

1) Safety

a) (b)(7)(E)  
b)  
c)

g. Take exit photographs

- 1) Exit photographs are used to settle claims of alleged damage caused by search, etc.
- 2) Ensure the photographs depict the entire scene as it appears when all search and collection is complete.

h. Release the scene

- 1) Only person in charge should have the authority to release the scene.
- 2) Once the scene is formally released, reentry may require a warrant.
- 3) Document, at minimum:

a) (b)(7)(E)  
b)  
c)

**Notes:**

4) Provide appropriate inventory to person to whom the scene is released in accordance with legal requirements.

i. Evidence Processing Report of Investigation

1) (b)(7)(E)



(b)(7)(E)

- a)
- b)
- c)

- 2) Report should fully identify and itemize all items of evidence which were recovered, their locations, condition, and the finder.
- 3) Document:

- a)
- b)
- c)
  
  
  
  
  
  
  
- d)
- e)
  
  
  
  
  
  
  
- f)
  
  
  
  
  
  
  
- g)

- 4) Reference the evidence as having been recorded on 6051S, provided line item numbers, and include 6051Ss serial numbers (top right-hand corner)
- 5) Document that all evidence was photographed in place and where the photos will be kept (i.e. the case file).
- 6) Report should identify that the items seized were seized as evidence and what was subsequently done with the items.



- a) Taken to the Lab and turned over to other law enforcement/delivered to CBP SPC and Evidence Vault/or placed in an HSI evidence room
- 7) Need to Fully Identify Persons at location where Evidence Recovered and specifically designating all Law Enforcement Personnel

**Notes:**

**D. EPO 4: Discuss procedures for storing evidence.**

- 1, All non-forfeitable evidentiary items must be turned over to the HSI SPS/Evidence Custodian immediately following the seizure of the items.
- 2. Seized property or evidence, including government-generated evidence, will not be permitted to be stored outside of an HSI certified seized property/evidence room (i.e., (b)(7)(E) [redacted])

(b)(7)(E) [redacted]

- a. HSI does not have (b)(7)(E) [redacted]

3. Storage of High-Risk Evidence:

- a. (b)(7)(E) [redacted]
- b. [redacted]
- c. [redacted]

4. Storage of Forfeitable Evidence:

- a. (b)(7)(E) [redacted]
- b. [redacted]



(b)(7)(E)

5. Storage of Non-Forfeitable Evidence:

a.

(b)(7)(E)

b.

c.

6. Storage of Government-Generated Evidence:

a.

(b)(7)(E)

b.

c.

d.

7.

(b)(7)(E)

8. Storage and Acceptance of Property in HSI Seized Property/Evidence Rooms:

- a. The HSI SPS must sign the original DHS Form 6051S (and DHS Form 6051A, if needed) upon receipt of evidence, release, and disposition if he or she was not the last person to sign the appropriate DHS Form(s) 6051.
- b. The HSI SPS must ensure that all seized property/evidence complies with the packaging, labeling, and storage requirements of the SAMEPH.





**Notes:**

**E. EPO 5: Discuss procedures for disposing of evidence.**

All seized property/evidence must be retained until the completion of all trial, appellate, or other judicial proceedings, or if the defendant becomes a fugitive prior to adjudication of the case. Work with AUSA or State/Local Prosecutor to ensure all evidentiary items needed for trial are available.

1. Disposing of Non-Drug Evidence:
  - a. Case agents should return property that is no longer needed as evidence to the owner or his or her designated legal representative within 10 working days.
  - b. Group Supervisor will close cases only after receiving a completed DHS Form 6051 and/or DHS Form 4613, "Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise."
2. Disposing of Forfeitable Evidence:
  - a. Local FP&F office will process all seized/forfeitable evidence.
  - b. Case agent must keep the AUSA apprised of the changing status of such property.
  - c. Case agents are also responsible for coordinating cases among the AUSA, the local FP&F office, and the Office of the Principal Legal Advisor, particularly when subsequent civil forfeitures of evidence are anticipated.
  - d. The disposition of seized/forfeitable evidence must be approved by the FPFO. Although HSI may store seized/forfeitable items for logistical purposes, only the FPFO can authorize their destruction and/or disposition.
  - e. Once disposition has been issued, the FP&F Paralegal Specialist will issue a DHS Form 7605 and/or DHS Form 4613 to the requesting case agent.
3. Disposing of Non-Forfeitable Evidence:



- a. Case agent is responsible for the disposition of all non-forfeitable seized property/evidence.
- b. Personal property (including non-forfeitable evidence) and/or documentary evidence may be destroyed only when the following conditions are true:
  - 1) All attempts to return the property/evidence to its owner or designated legal representative have failed.
  - 2) All judicial aspects concerning the seized property/evidence have been completed.
  - 3) There are no fugitives remaining in the investigation.
- c. After the above coordination steps have been taken and attempts have been made to return seized evidentiary items to their owners, the case agent and/or HSI SPS/ Evidence Custodian may destroy the property in the presence of two witnesses, preferably the case agent and another SA familiar with the case.
- d. Case agent's first-line supervisor, case agent, and witnesses must sign the DHS Form 4613 in the designated blocks.
- e. The original DHS Form 4613 must be placed in the investigative case file, and copies provided to the HSI/CBP SPS and FP&F.

**Note:**

(b)(7)(E)

(b)(7)(E)

- 4. Disposition of Abandoned Property
  - a. This disposal will be in accordance with 41 C.F.R. Part 101-48, "Utilization, Donation, or Disposal of Abandoned and Forfeited Personal Property," and after the following steps have been taken:
    - 1) Attempts have been made to notify the defendants in writing at their last known address (residential and/or place of incarceration) that their personal effects will be destroyed within 30 days if not claimed. These attempts should be completed using return receipt, which will be placed in the investigative case file along with a copy of the written notification.
    - 2) The property has been inventoried on a DHS Form 6051S (and DHS Form 6051A, if needed).
    - 3) The AUSA and the defendant's attorneys have been notified in writing that the property will be destroyed within 30 days if not claimed. These attempts should also be completed using return receipt, which will be placed in the investigative case file along with a copy of the written notification.
  - b. If the case agent is unable to return the evidence to the owner or designated representative, the SAC or designee may order the property destroyed and issue an "Order to Destroy and Record of Destruction of Forfeited, Abandoned, or Unclaimed Merchandise" (DHS Form 4613).



5. Disposition of Purchased Evidence Owned by the Government
  - a. When purchased evidence is no longer needed, purchased items that are not subject to forfeiture should be reported to GSA in accordance with 41 C.F.R. § 102-36, "Disposition of Excess Personal Property."
  - b. Firearms, ammunition, and other related weapons accessories acquired through POE will be properly disposed of through the OFTP AOB. The disposition of firearms is governed by regulations under 41 C.F.R. § 101-42.1102-10 and the Interim ICE Firearms Policy, dated July 7, 2004, or as updated or superseded.
  
6. Disposition of Government-Generated Evidence (Original Recordings)
  - a. All recordings entered into evidence in a hearing or trial shall not be destroyed except upon an order from the issuing judge.
  - b. When evidence media is destroyed, it shall be rendered unusable and unrecoverable and documented on a DHS Form 4613.
    - 1) Work with CFAs to determine which method to use for rendering media unrecoverable
      - a) Can provide guidance in the destruction of media
      - b) Can conduct a "forensic wipe" of seized/forfeited machines

**Note:** See Section 17.27 of the Technical Operations Handbook (HSI HB 14-04), dated July 21, 2014, or as updated.

**Notes:**



## Demonstration

(b)(7)(E)

## Student Practice

Refer to the Evidence Processing Lab Plan – it will be used as the Student Practice.



## CONCLUSION

### Summary of Main Ideas

SAs make many decisions concerning searches and seizures in the field and, frequently cannot consult reference materials, policy documents, or seek legal advice from their local Office of the Chief Counsel (OCC) or the appropriate U.S. Attorney’s Office (USAO). SAs must also recognize the importance of evidence collection and preservation, storage, and the final disposition of evidence seized in the field as required by policies and procedures.

### Integration

In this lesson, students learned the basics of collecting evidence. Students will practice identifying, collecting, and processing evidence in the Evidence Processing lab.

### Objectives

After completing this lesson, students are now able to:

- Discuss the main objective in processing evidence.
- Provide an overview of terminology, seizure authority, forms used, and roles and responsibilities involved in the seizure process.
- Explain the process for evidence recovery and seizure from the pre-search planning phase to the post-search activities.
- Discuss procedures for storing evidence.
- Discuss procedures for disposing of evidence.

### Motivation

Searches and seizures consistent with Fourth Amendment protections are complex subjects for SAs. HSI search and seizure methods conform to constitutional and statutory limitations involving border operations and operations conducted in the interior of the United States. Statutes, regulations, and case law, including Supreme Court decisions, do not address every factual scenario. SAs also know the prosecutorial policies in their particular districts.

SAs make many decisions concerning searches and seizures in the field and, frequently, cannot consult reference materials, policy documents, or seek legal advice from their local Office of the Chief Counsel (OCC) or the appropriate U.S. Attorney’s Office (USAO). It is important to understand and apply the principles of search and seizure laws, policies, and procedures. SAs must also recognize that search and seizure law is intricate and continually evolving.

When executing warrants, (b)(7)(E)

(b)(7)(E)



## Test or Final Activity

In teams, students will plan and conduct a search for evidence in the Evidence Processing lab. The instructor will evaluate the team's performance based on the detection, collection, and required processing as presented in this lesson. The test for the evidence processing lesson occurs during Practical Exercise 2.



**Forging a New Legacy**

# **Homeland Security Investigations**

**Evidence Processing**

**HSI Special Agent Training**

**ICE Academy**

# Homeland Security Investigations (HSI)

## Terminal Performance Objective

Given a search warrant execution scenario, a set of case-related facts, and the presence of potential evidence, collect and process evidence in accordance with the Homeland Security Investigations Evidence Handbook HSI HB 15-05 / November 9, 2015, and in manner which qualifies that evidence to be admitted in future criminal justice proceedings under the Federal Rules of Evidence.



# Homeland Security Investigations (HSI)

## Enabling Performance Objectives

- Discuss the main objective in processing evidence  
Provide an overview of terminology, seizure authority, forms used, and roles and responsibilities involved in the seizure process  
Explain the process for evidence recovery and seizure from the pre-search planning phase to the post-search activities  
Discuss procedures for storing evidence  
Discuss procedures for the disposition of evidence

# Homeland Security Investigations (HSI)

## Review of the Past

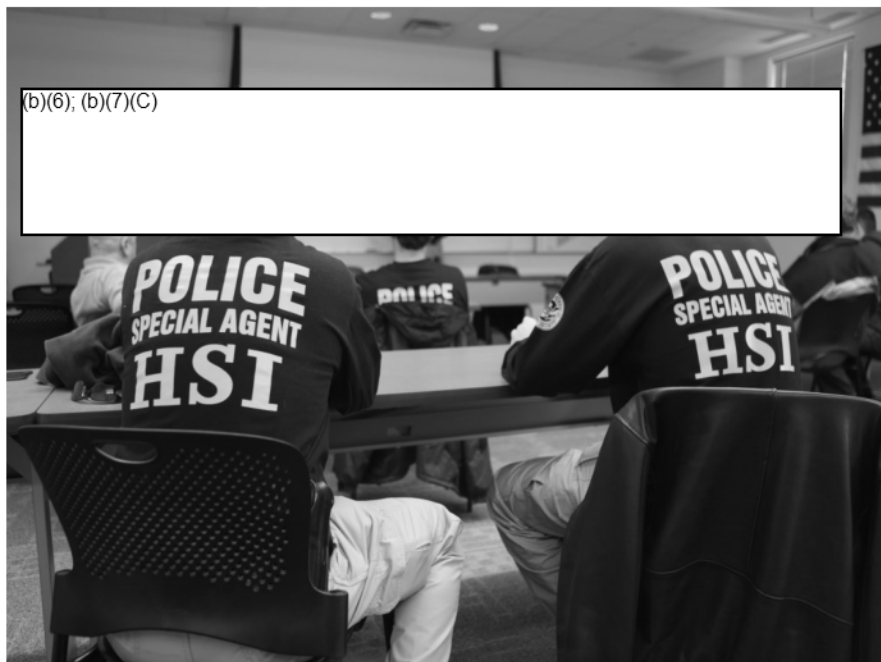
**CITP:**  
Conducting  
Searches and  
Documenting  
Evidence  
Recovery

**LEGAL:** Rea  
sons for  
Evidence  
Recovery  
and  
Handling  
Procedures

**AUTHORITY:**  
FRCP Rule  
41 and HSI  
Related  
Seizure  
Authorities

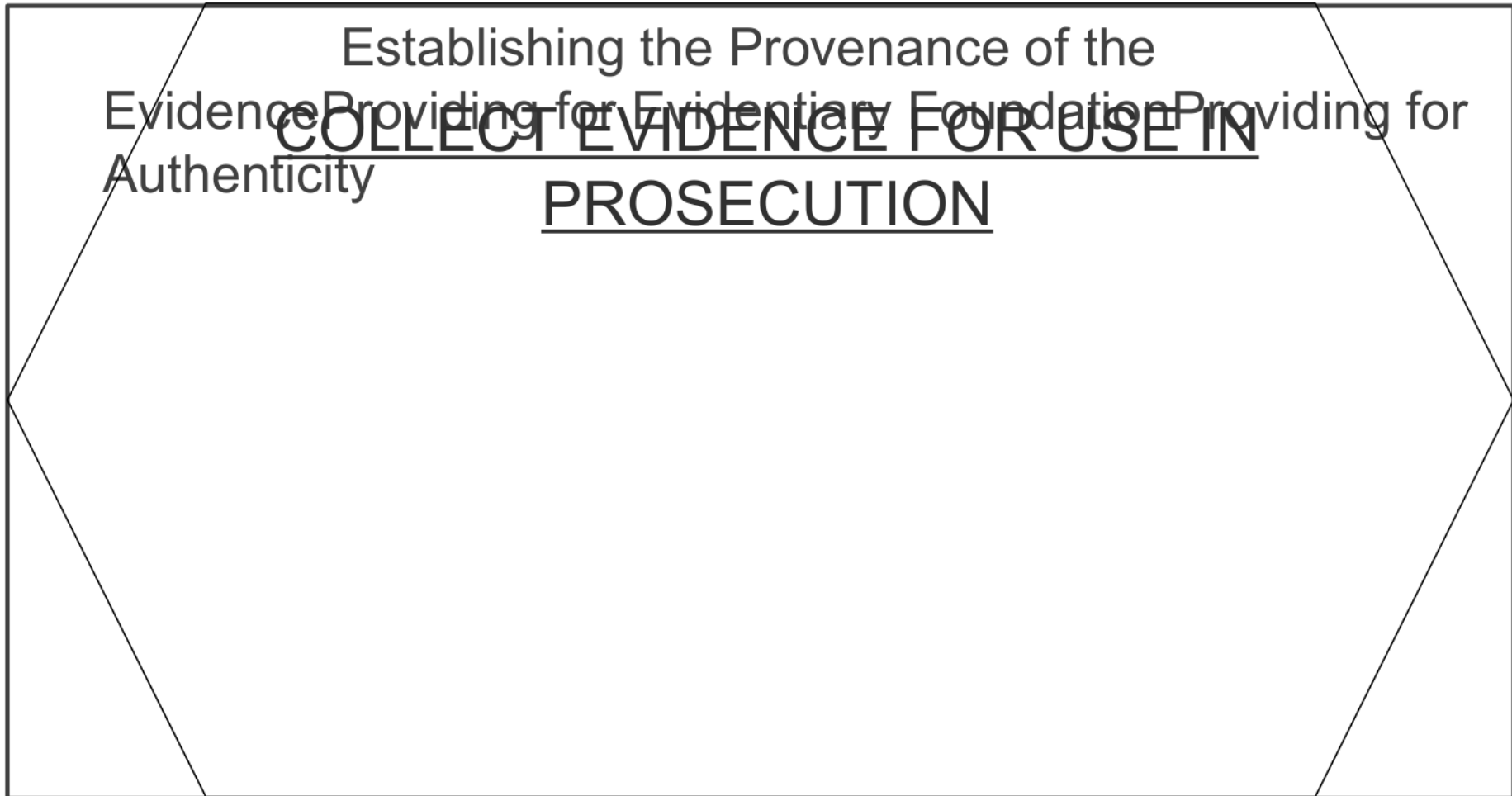
# Homeland Security Investigations (HSI)

## Agenda



# Homeland Security Investigations (HSI)

## Main Objective of Processing Evidence



# Homeland Security Investigations (HSI)

## Evidence: Need to Establish Admissibility

- Foundation – Provenance of Evidence, Authenticity, and Relevance  
SA must be able to testify to foundational/authenticity questions  
Can only be done by the Finder – first discovered evidence item  
Must be able to “recognize” item of evidence  
Must be able to testify as to how they recognize the item  
Must be able to testify in detail as to where the item was located and in what condition  
Must be able to testify that item as it is presented during the prosecution is “in substantially the same condition” it was when it was first discovered

# Homeland Security Investigations (HSI)

## Terminology

**Abandonment** – Abandoned property for which owner has voluntarily relinquished rights and ownership

**Detention** – Delaying the release of property pending a review of admissibility or importation/exportation

**FP&F** –  number generated by SEACATS for tracking seized and forfeited property

**Forfeitable Evidence** – Seized property, subject to forfeiture and needed as evidence

**Forfeiture** – Legal transfer of property ownership from owner to the U.S. government

# Homeland Security Investigations (HSI)

## Terminology (cont'd)

**Government-Generated Evidence** – Evidence obtained via investigative means

**High-Risk Evidence** – Controlled substances, weapons, and monetary instruments

**Incident Number** –  number generated by SEACATS for tracking and enforcement action type

**Non-Forfeitable Evidence** – Seized property that is not subject to forfeiture

**Purchase of Evidence (POE)** – Tangible items purchased with government funds during an investigation

# Homeland Security Investigations (HSI)

## Terminology (cont'd)

**Real Property** – Land and anything growing on, attached to, or erected on it

**SEACATS SAS** – Records statistical and enforcement information related to searches, arrests, and seizures

**SEACATS** – System of records for tracking seized and forfeited property

**Seizure** – Taking possession of property by legal right

**TECS** – System through which Case Management can be accessed

*TECS has been replaced with ICM*



# Homeland Security Investigations (HSI)

## DHS Evidence Forms – Evidence Custody Docs

- **6051S, Custody Receipt for Seized Property/Evidence – Documents property seized**  
**6051A, Custody Receipt for Detained or Seized Property/Evidence – Continuation sheet and attachment for additional seized items**  
**6051R, Receipt for Property – Documents and tracks return of property not identified on SEACATS SAS report**  
**6051WT – Identifies weapons**  
**6051D, Detention Notice and Custody Receipt for Detained Property – Documents property pending review for admissibility or importation/exportation**

# Homeland Security Investigations (HSI)

## Roles and Responsibilities

### **Seized Property Manager (SPM)**

Accountable for the security, handling, and inventory of seized and forfeited property

### **HSI Seized Property Specialist (SPS)**

Ensure the preservation, safeguarding, and disposition of all seized property/evidence released to their custody

**Evidence Custodians Responsible for the management of seized property/evidence rooms**

# Homeland Security Investigations (HSI)

## Roles and Responsibilities (cont'd)

**Seizing Special Agents Ensure the timely and accurate completion of the SEACATS SAS report and case initiator forms**

**Case Agents Ensure accurate inventory, storage, and disposition of seized property; input data into SEACATS and complete Form 6051**

# Homeland Security Investigations (HSI)

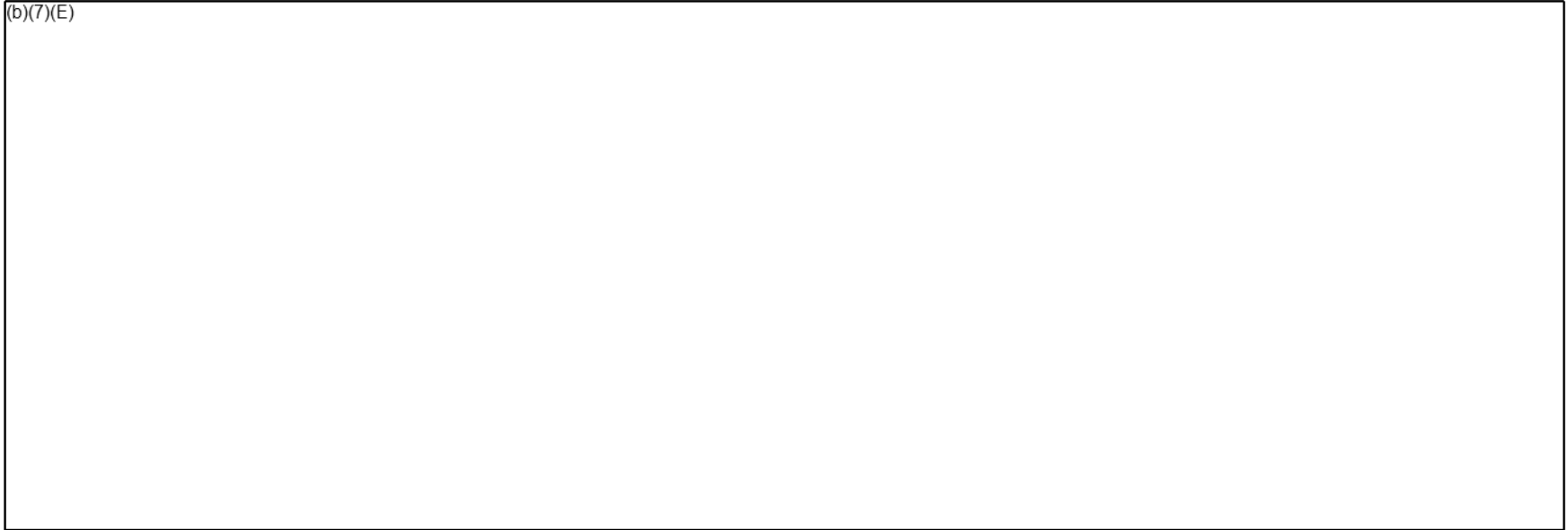
## Search Warrant Planning Considerations

- (b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant Planning Considerations

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Pre-Search Planning

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant Procedure

- (b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant Execution

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Search Warrant Execution & Evidence Processing

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant Execution & Evidence Collection

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Evidence Collection/Preservation

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

# Homeland Security Investigations (HSI)

## Laboratory Resources

- HSI Forensic Laboratory Questionnaire  
Section Latent Print Section Digital Program Polygraph Program CEIS  
Supports CBP and HSI personnel in various field laboratory tests and seized property/evidence DEA seized controlled substances  
USSS Laboratories – Multi-Faceted; Great Secondary Option

DEPARTMENT OF HOMELAND SECURITY  
U.S. Immigration and Customs Enforcement  
REQUEST FOR LABORATORY EXAMINATION  
PROPERTY LABORATORY  
HEADQUARTERS  
1000 MONTGOMERY AVENUE, SUITE 300  
FALLS CHURCH, VA 22044-7000  
800-735-5275  
WWW.ICTD.HQ.DHS.GOV

ICE Form 73-003  
Request for Laboratory Examination

Section I: SUBMITTER INFORMATION  
Name: \_\_\_\_\_ Title: \_\_\_\_\_  
Department/Agency: \_\_\_\_\_ Office: \_\_\_\_\_  
Program and Office: \_\_\_\_\_ File Number: \_\_\_\_\_  
Address: \_\_\_\_\_  
City/State/Zip: \_\_\_\_\_

Section II: CASE INFORMATION  
A. Type of Case:  Criminal  Civil  Other  
B. Is the subject currently in the custody of ICE?  Yes  No  
C. Submission Category:  Latent Print  Digital  Polygraph  CEIS  
D. Case Number: \_\_\_\_\_  
E. Agency Case Number: \_\_\_\_\_  
F. User Registration Number: \_\_\_\_\_  
G. Headline Number: \_\_\_\_\_  
H. Chain of Custody Serial Number: \_\_\_\_\_

Section III: EXAMINATIONS REQUESTED  
I. Latent Print Examination:  Yes  No  
II. Digital Examination:  Yes  No  
III. Polygraph Examination:  Yes  No  
IV. CEIS Examination:  Yes  No

Section IV: REMARKS  
Remarks: \_\_\_\_\_

iments

ICE Form

73-003

laboratories –

acting

tions of

atory – For

laboratories –

Multi-Faceted; Great Secondary Option

# Homeland Security Investigations (HSI)

## Evidence Identification

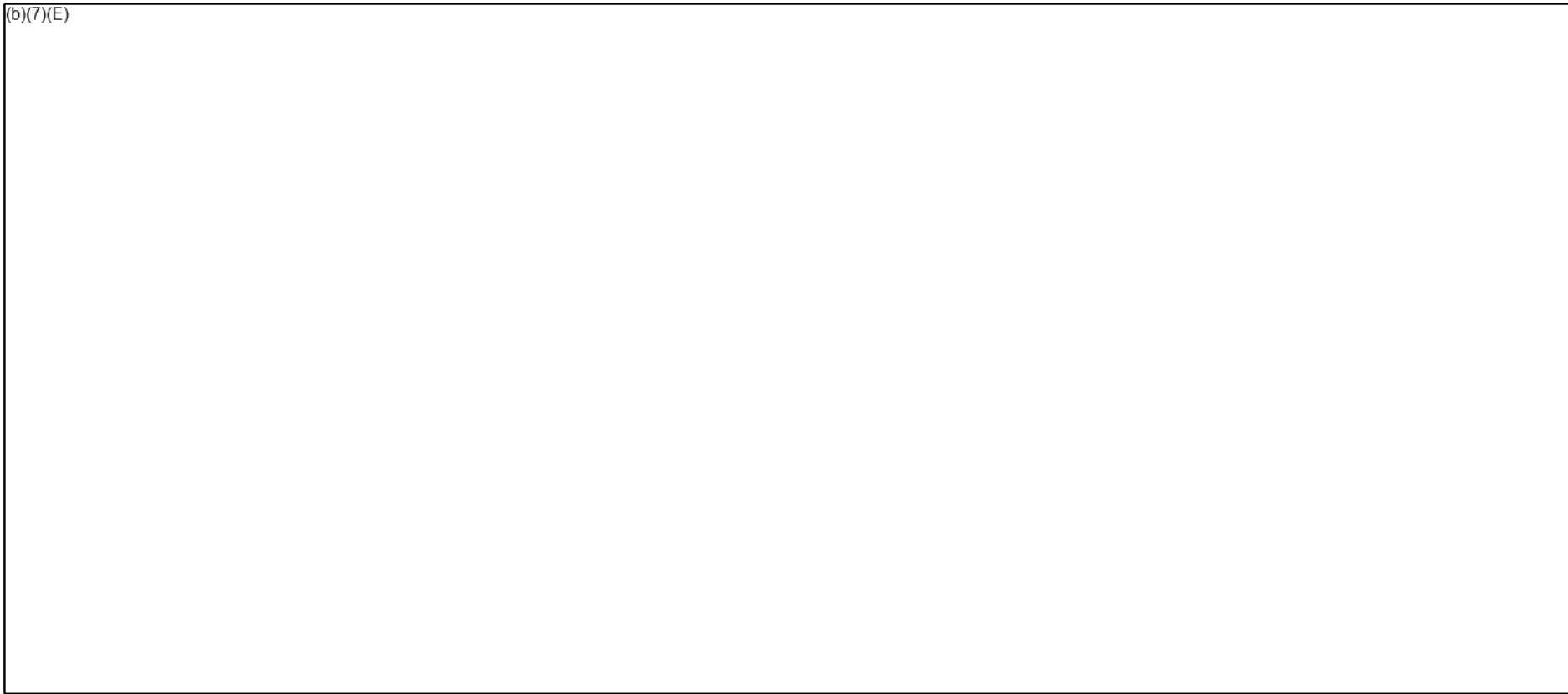
- Evidence includes Instrumentalities and Fruits Covered in Attachment B of Warrant Foundation/Authenticity Preserved (use of “Finder’s Note” – Index Cards) No Commingling Packaging/Labeling Evidence: containers must have evidence labels, DHS Form 366A.



# Homeland Security Investigations (HSI)

## Demonstration

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Classroom Exercise

(b)(7)(E)

Page 2280

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2281

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2282

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2283

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2284

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2285

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2286

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2287

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2288

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 2289

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act





# Homeland Security Investigations (HSI)

## Demonstration 1 – Part 1

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Types of Evidence

- Documentary  
Contraband/Counterfeit  
Weapons and Ammunition  
Currency and Negotiable Instruments  
Controlled Substances  
Latent Trace Biological  
Tool Markings  
Impression Electronic/Digital

# Homeland Security Investigations (HSI)

## Documentary Evidence

Documentary Evidence Includes indicia, notes, journals, commercial paperwork, and financial records  
Travel and Identification Documents  
Genuine Documents used in Fraud or by Impostor  
Review ASAP: Return seized documents not required as evidence to Owner



# Homeland Security Investigations (HSI)

## Contraband/Counterfeit

- Fraudulent Travel/ID Documents “Fraud Docs”  
Counterfeit Documents Fictitious Documents Altered Documents  
CBP Document Lab Other Types IPR  
Infringement Items Child Pornography

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

# Homeland Security Investigations (HSI)

## High Risk Evidence – 3 Types

- Controlled Substances  
Money  
Firearms\*\*  
HSI Prohibited by Policy from holding High Risk Evidence for more than 72 hours\*\*



# Homeland Security Investigations (HSI)

## Controlled Substances

- Seized Asset Management and Enforcement Procedures Handbook (SAMEPH) Chapter 11 – ICE Related Seizures 11.9.6 – Controlled Substances

(b)(7)(E)

(b)(7)(E)

with 6051 28 CFR

50.21 Procedure Policy vs. Reality



Page 2298

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2299

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2300

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2301

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

# Homeland Security Investigations (HSI)

## Bulk Marijuana



Bulk Marijuana 1KG – Threshold Amount  
Representative Sample/Exemplar for  
testing Threshold and Aggregates = Suff  
Current Criminal Evidentiary Practice SAMEPH –  
11.9.6 (References SAMEPH 4.1.18)

(b)(7)(E)

(b)(7)(E)

Page 2303

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2304

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act



Page 2305

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

Page 2306

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

# Homeland Security Investigations (HSI)

## Monetary and Negotiable Instruments

- Money is the ONLY Fundible evidence. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Currency Seizures - Considerations

(b)(7)(E)

Page 2309

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

# Homeland Security Investigations (HSI)

## Weapons and Ammunition

- Forfeit if: USED in violation of federal law  
USE in commission of a crime  
PURCHASED with criminal  
derived funds/proceeds  
Notify FP&F of Intent to  
Administrative Forfeit – 30 Days  
Return to legal owner  
if not forfeited or needed as evidence  
Encountered at Scene – Conduct



(b)(7)(E)

# Homeland Security Investigations (HSI)

## Weapons and Ammunition - Considerations

- ATF – E-Trace 18 USC §922(g)(5) Disposal via Abandonment = Method of Last Resort If not legally owned, must be stored as non-forfeitable until federal or state prosecution determined



# Homeland Security Investigations (HSI)

## Electronic Devices and Digital Media

- Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure authorizes seizure of electronic storage media  
General Rule: (b)(7)(E)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Special Categories: Purchased Evidence (POE)

- Forfeiture UNNECESSARY Title of Purchased Evidence Transferred with Payment Schedule I and II Controlled Substances ONLY POE items that MUST be entered into SEACAT Turned over to CBP

SPS

(b)(7)(E)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Special Categories: Government Generated Evidence

- Should not be entered on a SEACATS SAS report Includes Evidence Obtained Pursuant to ECPA Search Warrants and Orders  
Accountability: Record on DHS Form 6051S  
Segregate from seized property  
Document and label electronic evidence and surveillance.  
Consider “Best Evidence” Rules: Do not erase original electronic media  
Preserve original notes, media, or transcripts.  
Store original recordings with the DTA or Evidence Custodian (per SAC Intra-office Policy).

# Homeland Security Investigations (HSI)

## Packaging and Sealing Considerations

- Evidence Preservation Biological/L  
possible Seal bag with Evidence in  
bag. Identify flammable, volatile, or  
evidence. Minimize number of LECs with custody of  
evidence. Maintain original bags
- Protect if  
ger, outer



# Homeland Security Investigations (HSI)

## Chain of Custody

- In offering “Real Evidence” at trial the Government is required to account for the custody of the evidence from the moment it reaches its custody until the moment it is offered in EvidenceCOC goes to weight; not admissibilityOriginal 6051S stays with evidence. Notate 6051S Number in all reports



# Homeland Security Investigations (HSI)

## Chain of Custody (cont'd)

- Separate 6051S for forfeitable and non-forfeitable evidence  
Separate 6051S for all evidence with different routes or locations  
Use separate 6051S for property line items that have different category and property type codes. Line item numbers and property descriptions on 6051S must match those in the SEACATS SAS report  
Seizing SAs may use a separate original DHS Form 6051S for each line item

# Homeland Security Investigations (HSI)

## Wrapping Up Search Warrant

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant Report of Investigation (ROI)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant ROI

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Search Warrant ROI (Cont).

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Search Warrant ROI (Cont'd)

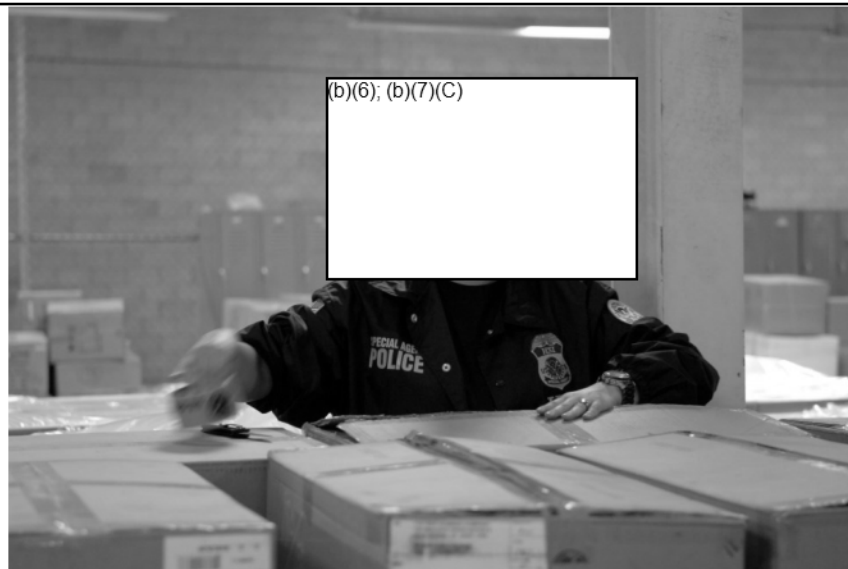
- (b)(7)(E)

# Homeland Security Investigations (HSI)

## Storing Evidence

- Includes “EV” Items (Non-Forfeitable) Turned Over to HSI SPS/Evidence Custodian Immediately Stored

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Storing – High Risk Evidence

- Do not store beyond 72 Hours Turn over to the CBP SPS



# Homeland Security Investigations (HSI)

## Storing Evidence – Forfeitable

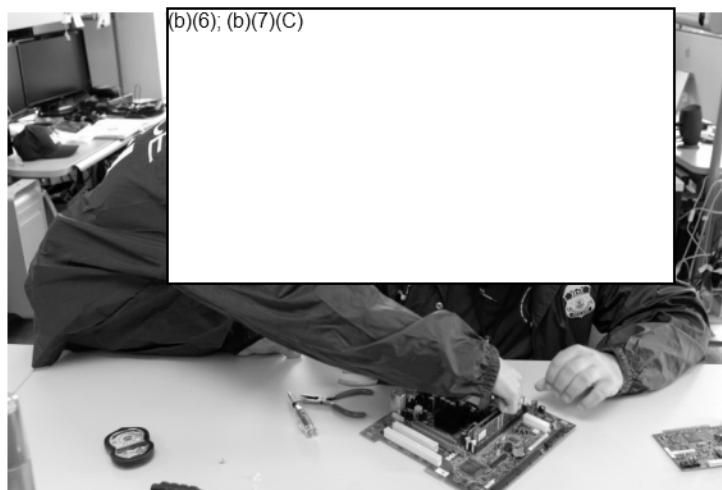
- “EN” Items Transferred to the CBP SPS by close of business within five business days of the date of seizure  
Exceptions are allowed with a written waiver from the AFU



# Homeland Security Investigations (HSI)

## Storing Evidence – Government-Generated

- Store IAW Field Office Policy: TEOs or HSI Evidence Room Segregate from any SEACATS Evidence Document using DHS Form 6051S (Tracking) Annotate: “Not in SEACATS” in Remarks Section



# Homeland Security Investigations (HSI)

## Disposing of Evidence

- Dependent on Prosecution and Appellate Concerns Should be returned as soon as possible when no longer required as evidence 10 working days guideline All Evidence needs to be disposed of prior to case closure SEACATS must be updated immediately All property records must be updated within three business days.





# Homeland Security Investigations (HSI)

## Disposing of Evidence – Non-Forfeitable

- Return to Party from Whom Seized Use 6051R (Receipt for Property) Destruction Order Signed by Group Supervisor Destruction Order provided to Evidence Custodian/SPS Executed by Case Agent with 2 Witnesses

# Homeland Security Investigations (HSI)

## Disposing of Evidence – Abandoned Property

- Abandonment – Relinquishment of Ownership Interest Disposed of via Destruction  
4613 Can be Retained IAW Management Regulations (148/102-41)

DEPARTMENT OF HOMELAND SECURITY  
ORDER TO DESTROY AND RECORD OF DESTRUCTION OF FORFEITED,  
ABANDONED, OR UNCLAIMED MERCHANDISE

ORDER TO DESTROY	
Debiture or General Order No., Etc.	Quantity and Description of Merchandise
Method of Destruction	
Authorizing DHS Officer	
Name _____ X _____ Signature	Date _____
RECORD OF DESTRUCTION	
DHS Officer	
Name _____ X _____ Signature	Date _____
Witnesses to Destruction	
Name _____ X _____ Signature	
Witnesses to Destruction	
Name _____ X _____ Signature	
Location	Method of Destruction

DHS Form 4613 (10/09)

# Homeland Security Investigations (HSI)

## Disposition of POE Items

- Firearms/Ammunition acquired through POE –  
Dispose according to OTTP AOBPOE Items for  
Government Use IAW 41 C.F.R. §102-36

# Homeland Security Investigations (HSI)

## Disposing of Evidence – Government-Generated

- Per SAMEPH: Recordings must be maintained for minimum of 5 years  
Recording entered into Evidence at Trial/Hearing  
Destruction requires court order  
Destruction Order for Media  
Media must be Unusable  
Data must be Unrecoverable

# Homeland Security Investigations (HSI)

## Demonstration 1 – Part 2

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Demonstration #1 – Part 3

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Demonstration 2 – Part 1

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Demonstration 2 – Part 2

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Summary

- Main Goal of Evidence Processing/Collection Search Activities – Support Evidence Collection Process Different Types of Evidence 3 High Risk Evidentiary Types Post Search – Reports Chain of Custody Evidence Disposition





Protecting the Borders Against Illicit Trade, Travel, and Finance



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





## 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 Register  
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. 1585  
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

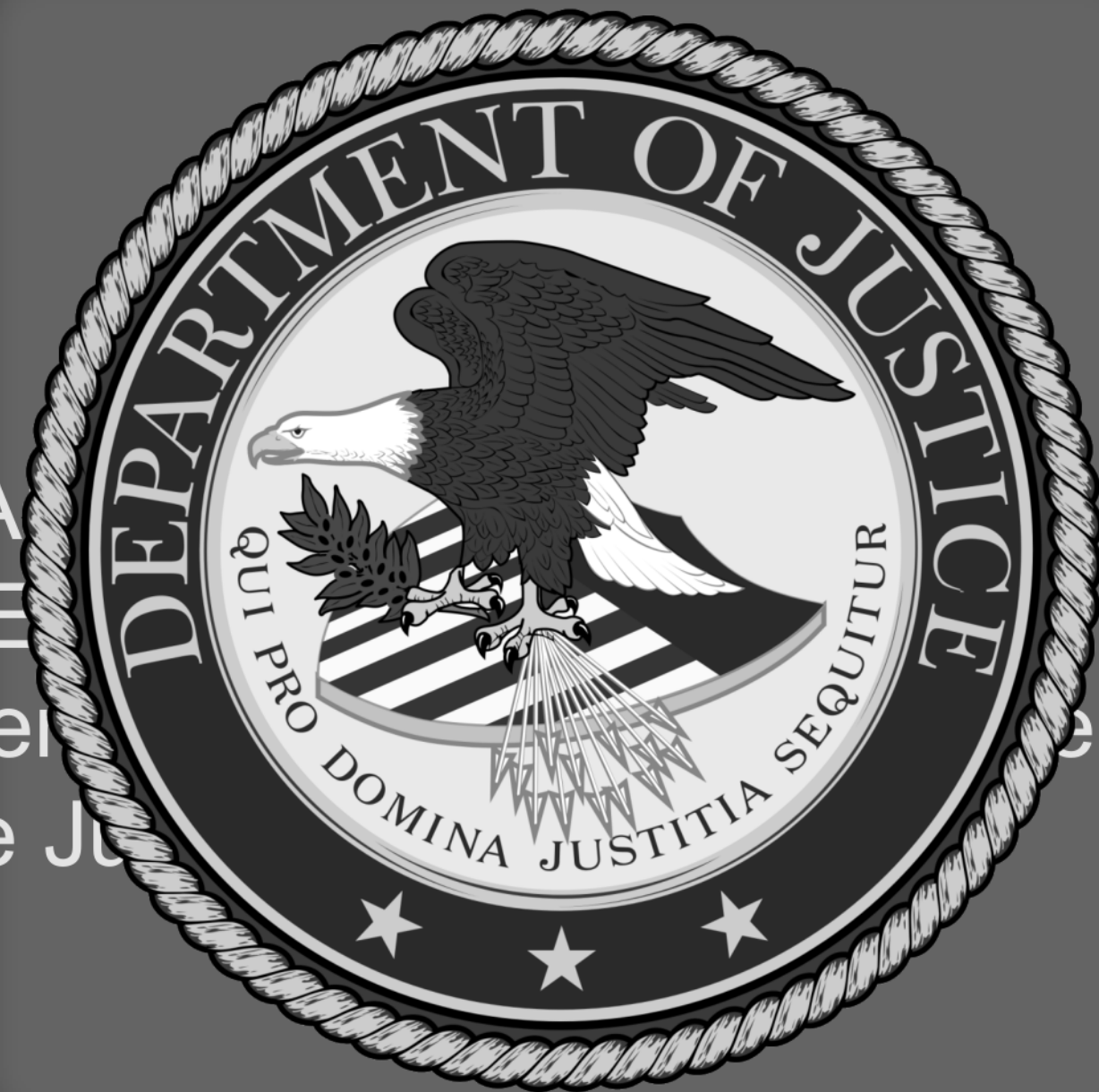
(b)(7)(E)







## 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 search  
and AUSA swear to the affidavit and application to the Judge  
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

**US Immigration and Customs Enforcement  
OFFICE OF TRAINING AND TACTICAL PROGRAMS**

**ICE Academy**



**TRACING OF ASSETS AND FORFEITURES  
11085**

**Student Guide**

**HSI Special Agent Training**

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). This contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.G. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, to anyone outside the ICE Academy, or to other personnel who do not have a valid "need-to-know" without prior approval of the ICE Office of Training and Tactical Programs Assistant Director or his designee.



## Tracing of Assets and Forfeitures

### Motivation

Seizures and forfeitures are some of the most powerful tools we have in the HSI arsenal. Asset forfeiture financially hurts the violator. Over the years, the emphasis has been shifting from merely putting the violator in jail to putting the violator in jail with no assets.

Ultimately the financial investigation should lead the Agent to locating assets derived from illegal activity. Subsequently, the assets should be seized and forfeited in concurrence with applicable forfeiture laws.

### Objectives

#### Terminal Performance Objective (TPO)

**Conditions:** Given case-related facts that indicate illicit assets and an example of a forfeiture proceeding (administrative, civil, or criminal),  
**Behavior:** determine the appropriate seizure/forfeiture procedure and asset tracing method,  
**Criterion:** to locate illicit proceeds and assets according to HSI guidelines in the Asset Forfeiture Handbook.

#### Enabling Performance Objectives (EPOs)

**EPO #1:** Explain methods of proving income.  
**EPO #2:** Identify sources of information to locate illicit proceeds and assets.  
**EPO #3:** Determine the difference between evidence and intelligence gathering.  
**EPO #4:** Describe terms, utilization of AIRG, and HSI policy/guidelines related to seizures and forfeitures.

### Review of the Past

You have had the Financial Investigations lesson and have conducted some preliminary financial investigations. Also, in CITP training, you received instruction about using the determining net-worth method of tracing illicit income. Legal lessons provided the statutory basis for seizing and forfeiting assets.

### Advance Organizer of Main Ideas

The HSI Asset Forfeiture Program exemplifies HSI's efforts to seize and forfeit assets that are associated with violations of federal law under HSI's investigative jurisdiction. This lesson provides a foundational understanding of the considerations pertaining to the seizing of tangible and nontangible assets and following the processes to ultimate forfeiture.



## Agenda

In this lesson, we will:

- Explain:
  - Methods of proving income
  - Sources of information to locate illicit proceeds and assets
  - Difference between evidence and intelligence gathering
  - Terms, utilization of AIRG, and HSI policies and guidelines related to seizures and forfeitures
- Demonstrate and practice identifying methods of tracing illicit income and procedures for conducting an investigation involving seizures and forfeitures.

## INSTRUCTION

### Explanation

#### A. EPO #1: Explain methods of proving income.

1. *Direct* – known and full documentation of specific transactional amounts are readily available

a. (b)(7)(E)

b. (b)(7)(E)

2. *Indirect methods* – Used when defendant has an unexplained display of wealth

a. Unexplained display of wealth – when there is:



- 1) (b)(7)(E)
- 2) (b)(7)(E)

b. SA must determine if the defendant derived the unexplained wealth through illegal, income-producing activities – contraband smuggling, ID and benefit fraud, export violations, etc.

c. Indirect tracing of illicit income

- 1) (b)(7)(E)
- 2) (b)(7)(E)

d. *Indirect tracing* – used for decades – for example, Al Capone’s conviction in the 1930s

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

e. How indirect methods prove illegal income

1) Three ways to dispose of income, both legal and illegal: (b)(7)(E)

- (b)(7)(E)
- (b)(7)(E)





(b)(7)(E)

- f. Three indirect methods of tracing illicit income – selection of particular method depends primarily on what would be easiest and clearest to use in a courtroom presentation to emphasize the major means of funds disposition.

(b)(7)(E)

Page 2370

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2371

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2372

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2373

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



2. (b)(7)(E)

3. Asset Identification Removal Groups (AIRGs)
- a. Expertise enabling HSI to identify, seize, and forfeit major violators' illegally derived assets, in concert with criminal investigations and prosecutions
    - 1) Primary mission to support asset removal of real property.
    - 2) Assist agents in asset identification and subsequent forfeiture.
  - b. AIRGs have expertise to:
    - 1) Identify assets with forfeiture potential
    - 2) Establish forfeiture provisions (civil/criminal)
    - 3) Establish probable cause for seizure

**Notes:**

**C. EPO #3: Determine the difference between evidence and intelligence gathering.**

1. There are many considerations concerning which assets to forfeit, and when to forfeit. During the course of an investigation, the case agent may obtain information that is only suitable as intelligence, instead of actionable information because of:

a. (b)(7)(E)

b.



2. To avoid common pitfalls:

(b)(7)(E)

**Notes:**

**D. EPO #4: Describe terms, utilization of AIRG, and HSI policy/guidelines related to seizures and forfeitures.**



1. Background of asset forfeiture
  - a. Asset forfeiture has become one of the most powerful and important tools used against all manner of criminals and criminal organizations from drug dealers to terrorists to white-collar criminals who prey on the vulnerable for financial gain.
  - b. Derived from the ancient practice of forfeiting vessels and contraband in Customs and Admiralty cases, forfeiture statutes found throughout the federal criminal code.
  - c. Forfeiture used to abate nuisances and to take the instrumentalities of crime out of circulation.
    - 1) Example: a boat or truck is used to smuggle illegal aliens across the border – we can forfeit the vessel or vehicle to prevent its use repeatedly for the same purpose
    - 2) Example: same is true for an airplane used to fly cocaine from Peru into Southern California
    - 3) Example: a printing press used to mint phony \$100 bills
  - d. Forfeiture takes the profit out of crime, and returns the property to the victims.
  - e. With forfeiture laws, SAs can separate the criminal from his profits, and any property traceable to it – remove the incentive others may have to commit similar crimes.
  - f. If the crime is one that has victims, SAs can use the forfeiture laws to recover the property and restore it to the owners far more effectively than restitution.
  - g. Forfeiture provides both a deterrent against crime and a measure of punishment for the criminal.
    - 1) Many criminals fear the loss of their vacation homes, fancy cars, businesses, and bloated bank accounts far more than the prospect of a jail sentence.
    - 2) In many cases, prosecution and incarceration are not needed to achieve the ends of justice – sometimes, return of the property to the victim and forfeiture of the means by which the crime was committed will suffice to ensure the criminal is punished.
2. Forfeiture
  - a. Divestiture of the illicit assets without compensation of property used in a manner contrary to the laws of the sovereign.
  - b. Merely illegal use alone does not automatically give government right to seize and forfeit.
  - c. Only if property forfeiture is specifically authorized by statute.
  - d. Must have express statutory authority before seizing or proceeding against property for forfeiture.





(b)(7)(E)

3. Forfeiture definitions

Terms and Definitions can be found at the end of the Student Guide.

4. Role of AIRG

- a. Has expertise in identifying and tracking assets in all HSI case categories.
- b. Identifies assets and investments that have been illegally acquired by individuals and criminal organizations.
- c. Establishes probable cause to seize and forfeit all property, real and personal, used and/or acquired as a result of criminal activity.
- d. Identifies, analyzes, traces, seizes, and forfeits criminal proceeds deposited into traditional and non-traditional financial institutions; traces and forfeits stocks, bank accounts, bonds, and other investments related to criminal activity.
- e. Dismantles known criminal organizations by targeting their financial infrastructure and seeking criminal, civil, or administrative actions to accomplish that mission.
- f. Develops sources of information that can provide leads and intelligence on criminal groups and how they attempt to legitimize their wealth.
- g. Collects and assesses intelligence on investment trends, modus operandi, and financial structures favored by criminal organizations.

AIRG help is requested as a (b)(7)(E). This is important to the setup of who gets stats later.

5. Collaboration on search warrants

- a. During drafting of any search warrant affidavits, AIRG SA and criminal case SA should coordinate efforts and be certain to include the authority to search for and seize financial documents.
  - 1) AIRG SAs should assist in the execution of all search warrants so that the AIRG can search for and obtain specific information pertaining to the location of assets and the monies/proceeds generated by the particular SUA being investigated.
- b. Since financial records are frequently stored as electronic media, AIRG SAs, in cooperation with the criminal case SA, should request the assistance of a Computer Forensics Agent (CFA) during the planning and execution of any search warrant.

1) (b)(7)(E)



- c. During execution of any search warrant that provides authority to search for and seize financial documents, SAs should attempt to locate and obtain:

(b)(7)(E)

- d. Constant coordination and communication between the criminal case SA, the AIRG SA, the criminal AUSA, and the asset forfeiture AUSA is extremely important.
- 1) No decisions should be made arbitrarily by a single SA or other entity.
  - 2) AIRG SAs should inform and seek the advice of all parties.

6. General guidelines

(b)(7)(E)



(b)(7)(E)

- h. Document all stages of the investigation in a detailed ROI.

**Notes:**

7. Evaluation of a property independent of a pre-seizure analysis

(b)(7)(E)

8. Pre-seizure planning

(b)(7)(E)



(b)(7)(E)

While in the planning stages, HQ AFU Chief has to approve seized property. When the property is valued over \$1million, the EAD has to approve the seizure. ***These guidelines do not include monetary instruments (HSI YHB 10-04,10.7.***

9. What is being seized?

(b)(7)(E)

**Notes:**



10. Calculating net equity

- a. SAs must obtain net equity information prior to seizing real property and businesses.

(b)(7)(E)

11. Seizure thresholds

- a. Pursuant to DOJ Asset Forfeiture Policy Manual Section D.1, dated 2016, and barring an overriding law enforcement purpose, net equity must exceed the following thresholds in order to justify a seizure:

(b)(7)(E)

- b. The USAO in the SA's district may require net equity amounts greater than the national thresholds.



- 1) It is the responsibility of each AIRG to know the local prosecutorial guidelines.

12. Treasury Executive Office of Asset Forfeiture (TEOAF)

- a. Administers the Treasury Forfeiture Fund (TFF).
- b. TFF established in 1992 as the successor to what was then the U.S. Customs Service Forfeiture Fund.
- c. TFF is the receipt account for the deposit of non-tax forfeitures made by the following member agencies:
  - 1) Criminal Investigation Division, Internal Revenue Service
  - 2) ICE
  - 3) CBP
  - 4) U.S. Secret Service
  - 5) U.S. Coast Guard

## DEMONSTRATION

(b)(7)(E)

Page 2383

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 2384

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



Page 2385

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



(b)(7)(E)

## CONCLUSION

### Summary of Main Ideas

Greed and the acquisition of material goods motivate many criminals. Therefore, the government's ability to forfeit property connected with violations of federal law can be an effective tool to reduce the temptation to cross the legal line.

Using seizures and forfeitures aims to undermine the economic infrastructure of a criminal enterprise that, often times, mirrors legitimate businesses. Businesses need cash flow to operate; and they generate a profit from the sale of their "product" or "services." The obvious difference is use of illegal means to generate profits. Asset forfeiture can remove the tools, equipment, cash flow, profit, and, sometimes, the product itself, from these operations, leaving the criminal organization powerless.

Collaborate with AIRG, AUSA, CFAs, FP&F in planning seizures. Make sure that the affidavit

(b)(7)(E)

Seizure value must meet threshold requirements.

### Integration

For any case in which the subject may have financially benefitted from violations of federal law, Special Agents should proactively look for any indications of accumulated assets. The AIRG can provide assistance with more refined techniques that can be used to establish grounds for forfeiture of those assets.



## Objectives

You are now able to:

- Explain methods of proving income.
- Identify sources of information to locate illicit proceeds and assets.
- Determine the difference between evidence and intelligence gathering.
- Describe terms, utilization of AIRG, and HSI policy/guidelines related to seizures and forfeitures.

## Motivation

Seizures and forfeitures are some of the most powerful tools we have in the HSI arsenal. Asset forfeiture financially hurts the violator. Over the years, the emphasis has been shifting from merely putting the violator in jail to putting the violator in jail with no assets.

Ultimately the financial investigation should lead the Agent to locating assets derived from illegal activity. Subsequently, the assets should be seized and forfeited in concurrence with applicable forfeiture laws.

Asset forfeiture is a powerful tool to combat criminal activity and other violations that threaten national security.

## Test or Final Activity

The material in this lesson will be tested in PE 2 and in Comp 2 exam.



### Term and Definitions

Equitable Sharing	Division and transfer of forfeited property, or proceeds from forfeited property, between government agencies, based on each agency's contributions to and participation in an investigation.
Encumbrance	Anything that affects or limits the title of a property, e.g., liens, mortgages, easements, leases, or restrictions.
Facilitation	Use of an asset in the commission of a crime or in furtherance of criminal or otherwise proscribed activity.
Final Order of Forfeiture	An order entered by the court in a criminal forfeiture proceeding, following the preliminary order of forfeiture and any ancillary proceedings, authorizing the Government to take ownership and dispose of a property. The final order takes into account any third-party rights, as well as the defendant's interest in the property – known in some judicial districts as an “amended order of forfeiture.”
Interlocutory Sale	The court-ordered sale of an asset prior to a final order or judgment of forfeiture. A court may authorize such an action in cases where loss of market value or physical deterioration of an asset has occurred or is imminent.
Lien	A legal claim against an asset, which is used to secure a loan and must be repaid if the asset is sold.
<i>Lis Pendens</i>	Latin for “suit pending.” A written notification, filed with a county recorder's office, indicating that a forfeiture action against the property is pending on behalf of the Government. The notice minimizes the potential for the transfer of ownership by alerting potential buyers or lenders that the title of the property is in question and any purchase of the property may result in the new owner being bound by the court decision.
Net Equity	The market value of an owner's unencumbered interest in an asset, i.e., the difference between the fair market value of an asset and the outstanding balance of liens against that asset.
Payment in Lieu of Forfeiture	A defendant's voluntary substitution of a monetary payment in place of the forfeiture of a particular asset.
Post- and-Walk	Process of delivering a warrant of arrest <i>in rem</i> to the owner of a real property and affixing a copy of the warrant to the property itself. Undertaken as part of a civil forfeiture action following the filing of a civil complaint for forfeiture.



Preliminary Order of Forfeiture	In criminal forfeiture proceedings, an order of the court, issued after the defendant is found guilty by a jury or enters a plea of guilty, which sets forth a money judgment or directs the defendant to surrender his or her interest in the property to the Government.
Pre-Seizure Analysis	A title search, appraisal, net equity analysis, cost/benefit analysis, and/or other services performed by the real property contractor at the request of an AIRG following the identification of a real property that may be subject to forfeiture.
Proceeds	Any property derived from or obtained or retained, directly or indirectly, through some form of unlawful activity, including the gross receipts of such activity.
Seizure Threshold	The amount of net equity that a criminal must hold in an asset before an AIRG SA may contemplate the seizure and subsequent forfeiture of that asset.
Turnover Order	A turnover order is an authorization, obtained from the state court with jurisdiction over the seizure, which authorizes the state or local agency to turn the seizure over to HSI for adoption.



**Forging a New Legacy**

# **Homeland Security Investigations**

**Confidential Informants**

**HSI Special Agent Training**

**ICE Academy**

# Homeland Security Investigations (HSI)

## Terminal Performance Objective

Given a set of case-related facts and a designated interaction with a potential Confidential Informant (CI), follow the policies and procedures that the HSI Special Agent must accomplish to successfully recruit, document, and compensate CIs, according to the HSI Informants Handbook



# Homeland Security Investigations (HSI)

## Enabling Performance Objectives

Discuss the primary considerations and strategies involved with the recruitment/cultivation of Confidential Informants (CIs)

Describe the management of HSI Confidential Informants

Determine CI File maintenance requirements

Discuss options for compensating CIs



# Homeland Security Investigations (HSI)

## Review of the Past

CITP  
training:  
learned  
about  
working  
with CIs



General  
experience

(b)(7)(E)



Legal: Rule  
16 of the  
Federal  
Rules of  
Criminal  
Procedure,  
“Discovery  
and  
Inspection”

# Homeland Security Investigations (HSI)

## Main Ideas

### Using CIs in the context of Homeland Security Investigations

- Define an informant or potential informant
- Minimize the risks involved when interacting with CIs
- Locate and adhere to the strict policies established in the HSI Informants Handbook

# Homeland Security Investigations (HSI)

## Agenda

Discuss the primary considerations and strategies for recruiting and cultivating CIs

Describe the management of HSI CIs

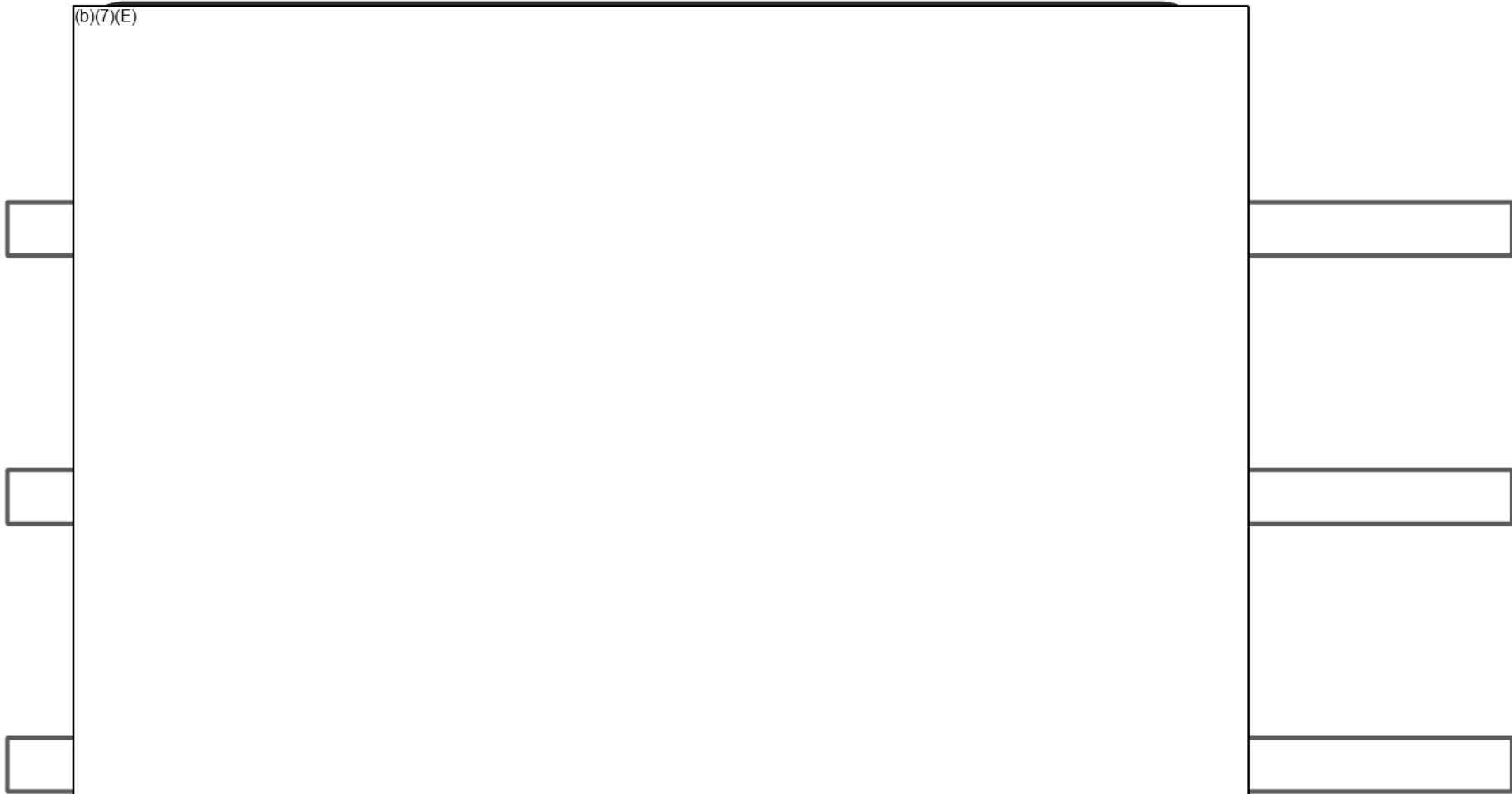
Determine CI File maintenance requirements

Discuss options for compensating CIs

# Homeland Security Investigations (HSI)

## Confidential Informants

(b)(7)(E)



Page 2397

Withheld pursuant to exemption

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

of the Freedom of Information and Privacy Act

# Homeland Security Investigations (HSI)

## Sources

Cooperating Defendants (CDs)

Confidential informants (CIs)

Sources of information (SOIs)



(b)(7)(E)



# Homeland Security Investigations (HSI)

## Cooperating Defendant

Provides HSI with credible information concerning unlawful activity. Required to have AUSA concurrence but functionally works under the direction and control of an HSI SA

Has no reasonable expectation of confidentiality

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Confidential Informant

Provides HSI with credible information concerning unlawful activity and works under the direction and control of an HSI SA

Has reasonable expectation of confidentiality

(b)(7)(E)





# Homeland Security Investigations (HSI)

## Source of Information

Provides information concerning unlawful activity to HSI without direct participation in investigation

Has a limited reasonable expectation of confidentiality

(b)(7)(E)



# Homeland Security Investigations (HSI)

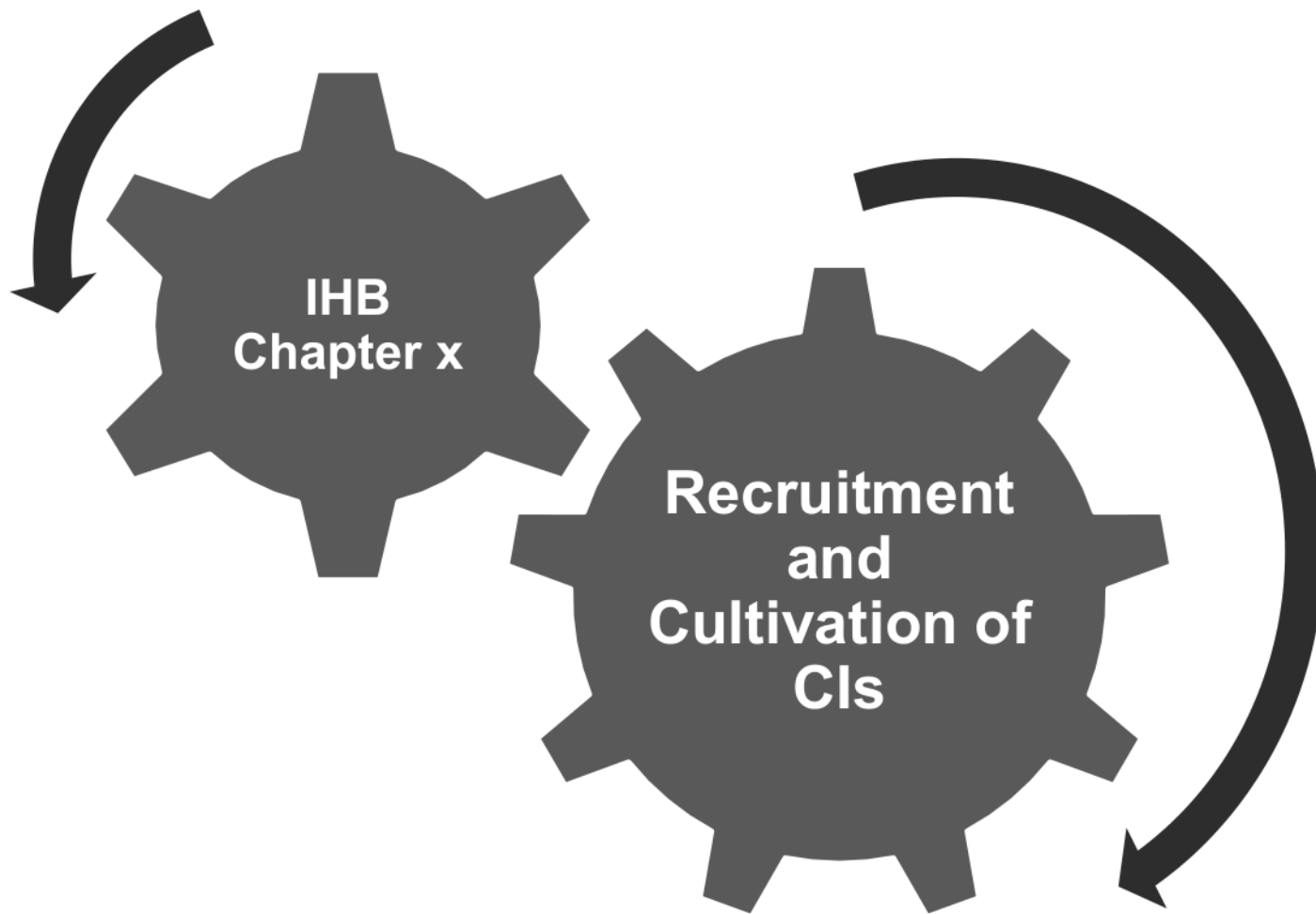
## Who Controls and Directs Sources

HSI SA acts as “Control Agent” – has the primary contact with a given CI

Other ICE/HSI employees can cultivate and develop informants **but** only SAs can document and control CIs

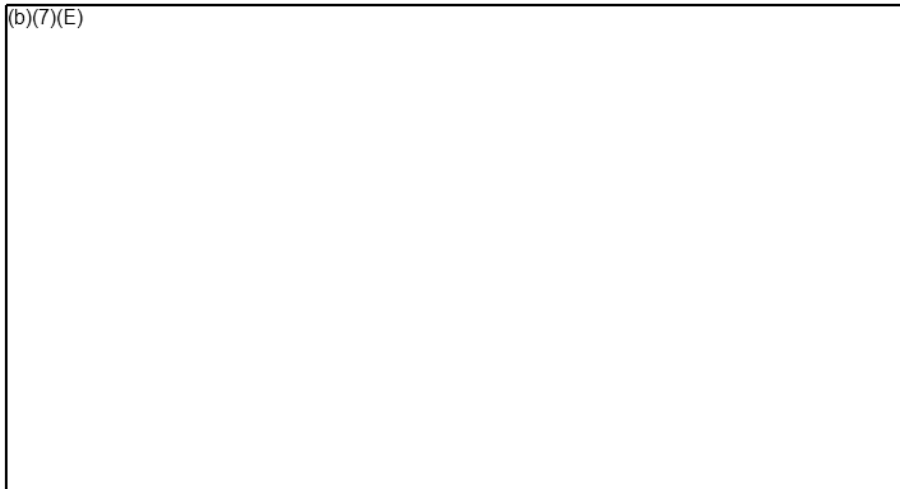
HSI TFOs can act as “alternate” (backup) control agents

# Homeland Security Investigations (HSI)



# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (1 of 8)



# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (2 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (3 of 8)

(b)(7)(E)



# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (4 of 8)

(b)(7)(E)

# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (5 of 8)

(b)(7)(E)





# Homeland Security Investigations (HSI)

## Prospective Informants/Sources (6 of 8)

(b)(7)(E)

