



# Certification Course Legal Training

b7E



b6  
b7C

Science and Technology Law Unit  
Office of General Counsel  
Federal Bureau of Investigation



# General Operational Guidelines



b7E



# Evidence/Intelligence Collection


b3  
b7E



## The Law

- **Title III & Electronic Communications Protection Act**
  - Title III, 18 USC sec. 2510, Omnibus Crime Control and Safe Streets Act, Commonly referred to as the Wire Tap Act
  - As amended by the ECPA, Title III prohibits the interception of wire and oral communications, and electronic communications.
  - Provides for criminal penalties and civil damages against anyone who “intentionally intercepts, endeavors to intercept” any covered communication.



## Title III Order

- Under Title III, the government may apply for a court order authorizing an interception. 18 U.S.C. §2516(1)
- Application must specify the offense being investigated, the nature and location of the facilities where the communications are to be intercepted, and a particular description of the communications sought to be intercepted. 18 U.S.C. § 2518(1)
- Standard: Probable cause to believe that a particular offense is being committed and that targeting the specified facility will yield communications concerning the offense. 18 U.S.C. § 2518(3)



## Title III Order (cont.)

- Good for up to thirty days. Extensions allowed, but same standard applies to extension. 18 U.S.C. § 2518(5)
- Required to “minimize” the interception unrelated to criminal activity. 18 U.S.C. § 2518(5)
- Requires a finding that normal investigative procedures are unlikely to be successful or are too dangerous. 18 U.S.C. § 2518(3)(c)
- Requires notice to the target within 90 days. 18 U.S.C. § 2518(8)(d)



## Interception v. Search

- Title III real time interception of electronic communications, e.g. [REDACTED]

[REDACTED]

b7E

- Collection of stored data – a search of memory



## Pen Register/ Trap and Trace

- Court ordered surveillance
- Government must certify that information is likely to be obtained by use or device “is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3122(b)(2)





## What is the Pen/Trap “addressing information”?

- **Dialing, Routing, Addressing, Signaling Information**
- **Transmitted by Instrument or Facility from which a Communication is Transmitted (pen)**
- **Identifies Originating Number or Other D/R/A/S or is Reasonably Likely to Identify the Source (trap)**
- **Utilized in Processing or Transmission of Communications**
- **Is not “Contents of any...Communications”**



## Limitation:

- Thou shall NOT collect the Contents of any communication
  - 18 USC sec. 3121 (c) – “use technology reasonably available to restrict . . . so as not to include the contents of any wire or electronic communications”
  - 18 USC sec. 3127 pen/trap definition: “shall not include the contents of any communication”



# Stored Communications & Records

## ECPA 18 USC SEC. 2701

- Content of communication in “storage”
- Subscriber Records
- Transactional Records



## Unauthorized Access to Stored Communications

- **18 USC § 2701 (Electronic Communications Protection Act)**
  - **Unauthorized access to communications in “electronic storage” (e.g., one user snooping in another’s inbox)**
    - intentionally access without authorization a facility through which an electronic communication service is provided and thereby obtain a wire or electronic communication while it is in electronic storage.
  - **Inapplicable when authorized by the Service Provider, §2701(c)(1)**
  - **Excepts conduct authorized by a “user” of that service with respect to a communication of or intended for that user. §2701(c)(2)**



## Disclosure of Stored Content & Records

- **General rule:** a public provider (e.g., an ISP) may not freely disclose the content or records of its customer's communications to others [18 U.S.C. § 2702]
- **Non-Public Providers may voluntarily disclose for any reason**



## Law Enforcement Exception

- 18 USC sec. 2703
- Required disclosure of customer communications (in electronic storage) or records
- Requires search warrant (FRCP 41), Federal subpoena, or Federal court order
- 180 day rule
- Notice to subscriber or customer



## What's a § 2703(d) Court Order?

- **“Articulable facts” order**
  - “Specific and articulable facts showing that there are reasonable grounds to believe that [the specified records] are relevant and material to an ongoing criminal investigation”
- **A lower standard than probable cause but higher than pen/trap**
- **Notice may be delayed: up to 90 days (may extend) to avoid flight, destruction of or tampering with evidence, witness intimidation, seriously jeopardizing an investigation**



## Nationwide Search Warrants for E-Mail:

- Investigators may use section 2703(a) warrants to compel disclosure of stored communications from providers anywhere in the country
- Issued “by a court with jurisdiction over the offense under investigation”
- Consistent with use of federal grand jury subpoenas and orders under section 2703(d).





## Basic Subscriber Information

**Can be obtained w/ Subpoena, 2703(d) order, or Search warrant**

### **Provider must give government:**

- Name, Address
- Local and long distance telephone connection records, or records of session times and durations;
- Length of service (including start date) and types of service utilized;
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and source of payment for such service (including any credit card or bank account number)



## Transactional Data

- **“A record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).”**  
§ 2703(c)(1) Everything that’s not content & not subscriber information
  
- **Example:**
  - Cell-site data;
  - Addresses / Identities of past e-mail correspondents
  - Incoming e-mail traffic information;
  - Account logs that record usage e.g., ULRs (web surfing activity)
  
- **Use § 2703(d) order to collect prospectively**



# CONTACT INFO



Assistant General Counsel  
Office of the General Counsel  
Science and Technology Law Unit



b6  
b7c



Wake up.  
It's time to leave.



# Certification Course Legal Training



Science and Technology Law Unit  
Office of General Counsel  
Federal Bureau of Investigation

b7E

b6  
b7C



# TOPICS

- **General guidelines**
- **The Law (e.g., Title III)**
- **Pen Register/ Trap and Trace**



- **Loan of ELSUR Equipment**

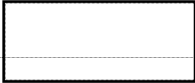


- **Stored Communications**
- **Computer Trespasser Exception**

b7E  
b3



# General Operational Guidelines



b7E



# General Operational Guidelines

- What is your legal authority?
- Why is it important?


b7E





# Law Enforcement Sensitive

- Law Enforcement Sensitive (LES) collection devices, systems, techniques, and related information are not to be disclosed. Only the product of the technical operation is disclosed.



b7E



# Law Enforcement Sensitive

- FOUO (For Official Use Only) – a caveat applied to sensitive but unclassified information that may be exempt from release under FOIA
- LES (Law Enforcement Sensitive) is another of 9 potential exemptions under FOIA to protect law enforcement sources and methods, evidence, reports, tools and techniques, etc.
- FOUO/LES is unclassified information



# Law Enforcement Sensitive

- Law Enforcement Sensitive (LES) equipment enjoys “qualified privilege”
- State/local vs. Federal prosecutions
- Testimony – how to ...


b7E



# The Law

## ■ Title III & Electronic Communications Protection Act

- Title III, 18 USC sec. 2510, Omnibus Crime Control and Safe Streets Act, Commonly referred to as the Wire Tap Act
- As amended by the ECPA, Title III prohibits the interception of wire and oral communications, and electronic communications.
- Provides for criminal penalties and civil damages against anyone who “intentionally intercepts, endeavors to intercept” any covered communication.



# Title III Order

- Under Title III, the government may apply for a court order authorizing an interception. 18 U.S.C. §2516(1)
- Application must specify the offense being investigated, the nature and location of the facilities where the communications are to be intercepted, and a particular description of the communications sought to be intercepted. 18 U.S.C. § 2518(1)
- Standard: Probable cause to believe that a particular offense is being committed and that targeting the specified facility will yield communications concerning the offense. 18 U.S.C. § 2518(3)



## Title III Order (cont.)

- Good for up to thirty days. Extensions allowed, but same standard applies to extension. 18 U.S.C. § 2518(5)
- Required to "minimize" the interception unrelated to criminal activity. 18 U.S.C. § 2518(5)
- Requires a finding that normal investigative procedures are unlikely to be successful or are too dangerous. 18 U.S.C. § 2518(3)(c)
- Requires notice to the target within 90 days. 18 U.S.C. § 2518(8)(d)



# Pen Register/ Trap and Trace

- Court ordered surveillance



- Government must certify that information likely to be obtained by use of device "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2)

b7E



# What is the Pen/Trap "addressing information"?

- Dialing, Routing, Addressing, Signaling Information
- Transmitted by Instrument or Facility from which a Communication is Transmitted (outgoing call) (pen)
- Identifies Originating Number or Other D/R/A/S or is Reasonably Likely to Identify the Source (incoming call) (trap)
- Utilized in Processing or Transmission of Communications
- Is not "Content of any...Communications"





# Limitation:

- Thou shall NOT collect the Contents of any communication
  - 18 USC sec. 3121 (c) – “use technology reasonably available to restrict . . . so as not to include the contents of any wire or electronic communications”
  - 18 USC sec. 3127 pen/trap definition: “shall not include the contents of any communication”

b3  
b7E



# Loan of ELSUR in Support of Federal, State, and Local Requests for Assistance

■ AG Order 2954-2008



b3  
b7E



# Stored Communications & Records

## ECPA 18 USC SEC. 2701

- "Electronic storage" is defined at 18 U.S.C. § 2510(17) as: (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication [REDACTED]

- For stored information, search warrant or 2703(d) order or subpoena with notice
- Under 2703(b) notice can be delayed

b7E  
b3



# Disclosure of Stored Content & Records

- **General rule:** a public provider (*e.g.*, an ISP) may not freely disclose the content or records of its customer's communications to others [18 U.S.C. § 2702]
- **Non-Public Providers may voluntarily disclose for any reason**



# Law Enforcement Exception

- 18 USC sec. 2703
- Requires disclosure of customer communications (in electronic storage) or records
- Requires search warrant (FRCP 41), Federal subpoena, or Federal court order (2703d order)
- 180 day rule
- Notice to subscriber or customer



# What's a § 2703(d) Court Order?

- **"Articulable facts" order**
  - "Specific and articulable facts showing that there are reasonable grounds to believe that [the specified records] are relevant and material to an ongoing criminal investigation"
- **A lower standard than probable cause but higher than pen/trap**
- **Notice may be delayed: up to 90 days (may extend) to avoid flight, destruction of or tampering with evidence, witness intimidation, seriously jeopardizing an investigation**



# Nationwide Search Warrants for E-Mail:

- Investigators may use section 2703(d) warrants to compel disclosure of stored communications from providers anywhere in the country
- Issued "by a court with jurisdiction over the offense under investigation"
- Consistent with use of federal grand jury subpoenas and orders under section 2703(d).



# Basic Subscriber Information

Can be obtained w/ Subpoena, 2703(d) order, or Search warrant, consent

Provider must give government:

- Name, Address
- Local and long distance telephone connection records, or records of session times and durations;
- Length of service (including start date) and types of service utilized;
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- Means and source of payment for such service (including any credit card or bank account number)





# Transactional Data

- "A record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)."  
§ 2703(c)(1) (Everything that's not content & not subscriber information)
- Example:
  - Cell-site data;
  - Addresses / Identities of past e-mail correspondents
  - Incoming e-mail traffic information;
  - Account logs that record usage e.g., URLs (web surfing activity)



## Title III (18 U.S.C. 2511-17) – Consent vs. Computer Trespasser Exception

- Need a court order to monitor the content of data communications – or an exception (consent).
- Content includes: [REDACTED]

[REDACTED]

b3  
b7E



# Relevant Exceptions to Title III



- Computer Trespasser exception.
- Consent of a party to the communication.
- Service Provider exception.



# Consent of a Party to the Communication – the Victim

## Computer

18 U.S.C. § 2511(2)(c)-(d)

Express consent

[Empty lined area for notes or details]



# Consent of a Party to the Communication – Banners

Implied consent

A large white rectangular area with horizontal lines, intended for notes or a list of items related to implied consent.

b5



## The Computer Trespasser Exception (18 U.S.C. §2511(2)(i))

### Requires:

- consent of the computer owner – authorization.
- the person performing the intercept must be “lawfully engaged in an investigation.”
- the person performing the intercept must have “reasonable grounds to believe the contents of the communications will be relevant to the investigation.”
- interception must be limited to communications “transmitted to, through, or from” the computer and MAY NOT capture communications other than those to or from the trespasser – broader than consent.



# The Computer Trespasser Exception (continued)

Legal tips:

A large white rectangular area with horizontal lines, intended for writing legal tips.

b5



# The Computer Trespasser Exception (continued)

Another legal tip:

A large rectangular area with horizontal lines, intended for handwritten notes or a legal tip.

b5





# The Computer Trespasser Exception (continued)

Practice tips:

A large rectangular area with horizontal lines, intended for writing practice tips.

b5



# Service Provider Exception ~~18 U.S.C. 2511(2)(a)(i)~~

- Authorizes interception or disclosure "while engaged in any activity which is a necessary incident to the rendition of service or the protection of the rights or property of the provider of the service"

[Redacted]

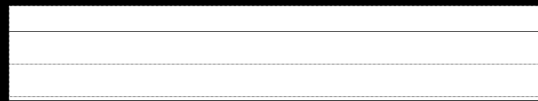
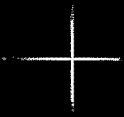
- Recommendation:

[Redacted]

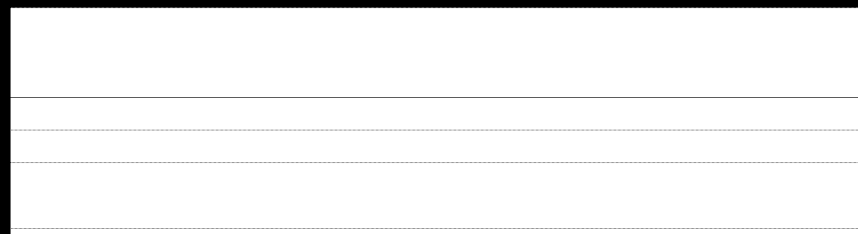
[Redacted]



# Questions?

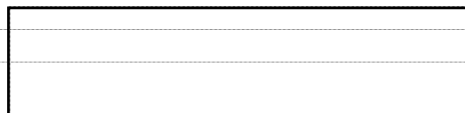


Assistant General Counsel  
Science & Technology Law Unit  
Engineering Research Facility  
Quantico, VA



b6  
b7C  
b7E

# Legal Fundamentals



b6  
b7c

Assistant General Counsel  
Science & Technology Law Unit  
Office of the General Counsel  
Federal Bureau of Investigation

# Agenda

- Real time monitoring of content
- Implied Consent/Banners
- Computer Trespasser
- International Issues
- Question and Answers

# General Operational Guidelines



b7E  
b3

# Compelled Disclosure under ECPA

## Evidence Sought

Undelivered email  
less than 180  
days old

Stored content

Most transactional  
Records (net flow data)

Basic subscriber  
info. and  
billing records

## Legal process

Search warrant

Subpoena or 2703 order  
with notice  
(or search warrant)

2703(d) order  
(or search warrant)

Subpoena  
(or 2703(d) order  
or search warrant)



**Current Issues and  
Procedures for Monitoring  
Content in Intrusion  
Investigations**



# Monitoring in Computer Intrusion Cases

Practice tips:

b3  
b7E

# Pen Register/Trap & Trace (18 U.S.C. §§3121-3172)

- Court order allows LE to collect signaling and routing information of communications (to, from, source/destination IP address, packet size, presence of attachments.
- Not content (e.g. real time collection of network flow data)
- Pen register – outgoing communications
- Trap & Trace – incoming communications

## Title III (18 U.S.C. 2511-17)

- Need a court order to monitor the content of data communications – or an exception.

- Content includes:

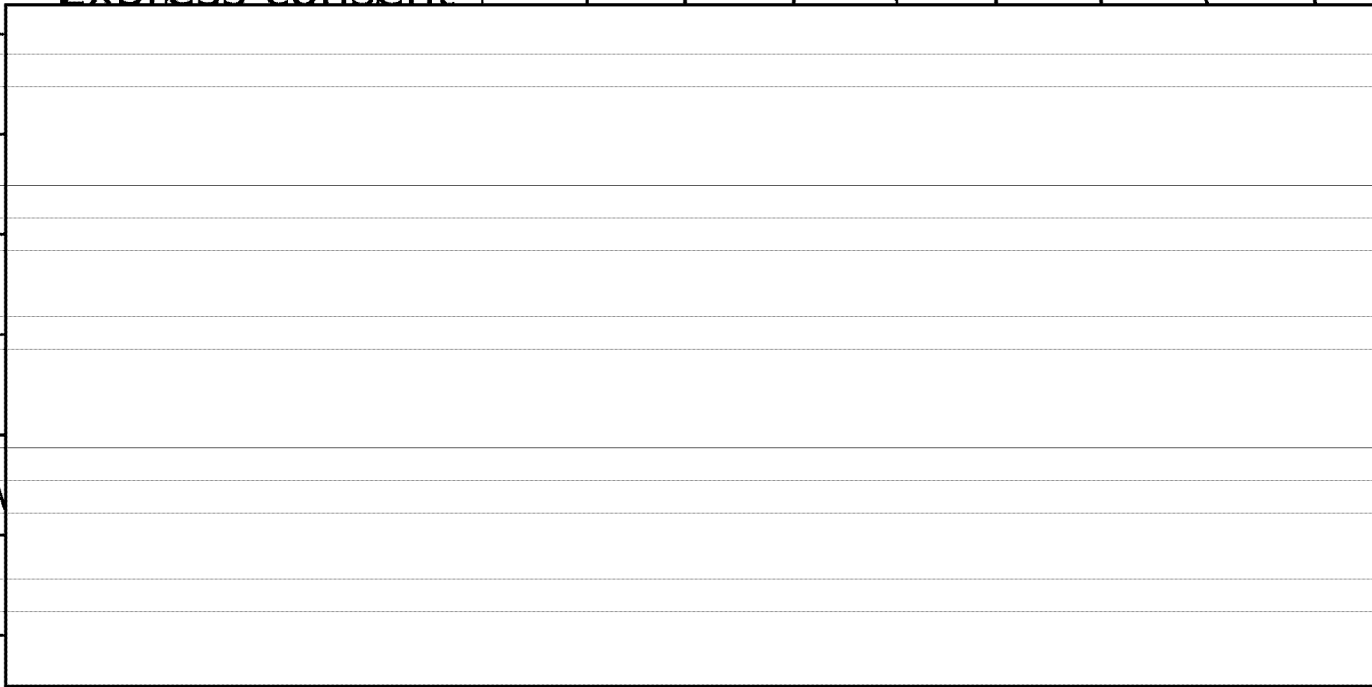
[Redacted content]

b3  
b7E

# Consent of a Party to the Communication the Victim Computer

18 U.S.C §2511(2)(c)-(d)

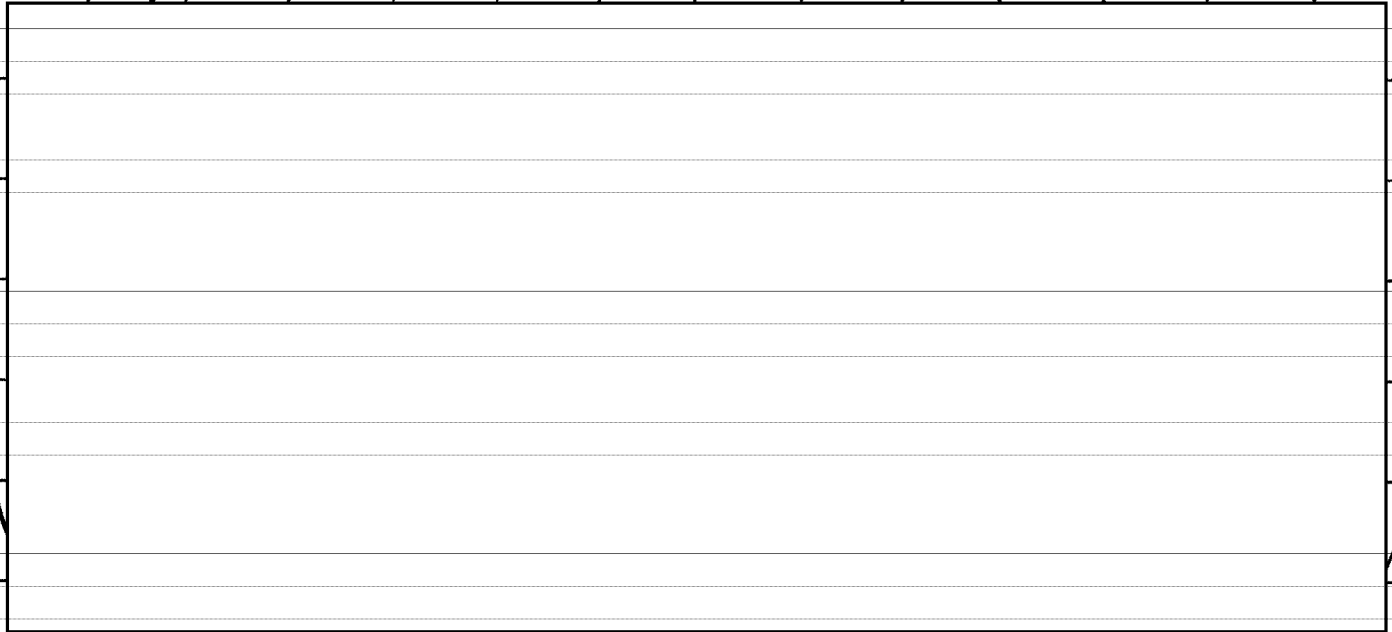
Express consent



b5

# Consent of a Party to the Communication – Banners

Implied consent



b5

# Relevant Exceptions to Title III

- Consent of a party to the communication.
- Computer Trespasser exception.
- Service Provider exception.

# The Computer Trespasser Exception (18 U.S.C. §2511(2)(i))

## Requires:

- consent of the computer owner – authorization.
- the person performing the intercept must be “lawfully engaged in an investigation.”
- the person performing the intercept must have “reasonable grounds to believe the contents of the communications will be relevant to the investigation.”
- interception must be limited to communications “transmitted to, through, or from” the computer and **MAY NOT** capture communications other than those to or from the trespasser – broader than consent.

# The Computer Trespasser Exception (continued)

Legal tips:





# The Computer Trespasser Exception (continued)

Another legal tip:



b3  
b7E

# The Computer Trespasser Exception (continued)

Practice tips:



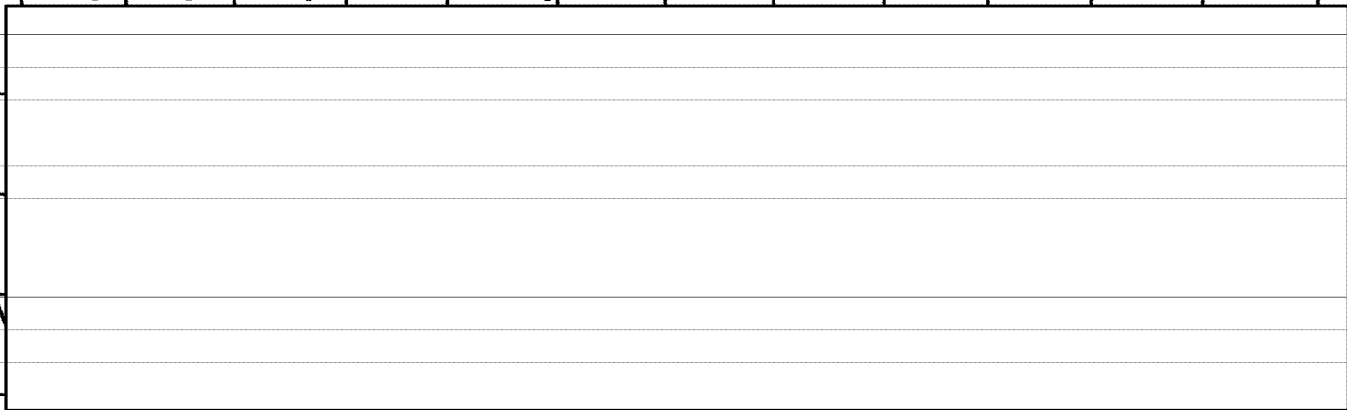
b3  
b7E

# Service Provider Exception

18 U.S.C. 2511(2)(a)(i)

- Authorizes interception or disclosure  
"while engaged in any activity which is a  
necessary incident to the rendition of  
service or the protection of the rights or  
property of the provider of the service"

b3  
b7E





# International Issues

# Legal Fundamentals Contact Information

Assistant General Counsel  
Science & Technology Law Unit  
Office of the General Counsel

b6  
b7C  
b7E

[Redacted]

# Program

[Redacted] DIVISION

[Redacted]

SSA [Redacted]

[Redacted]

b6  
b7C  
b7E

[Redacted]

- SA [Redacted]

- SA [Redacted]

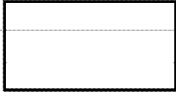
- SA [Redacted]

- SA [Redacted]

- SA [Redacted]

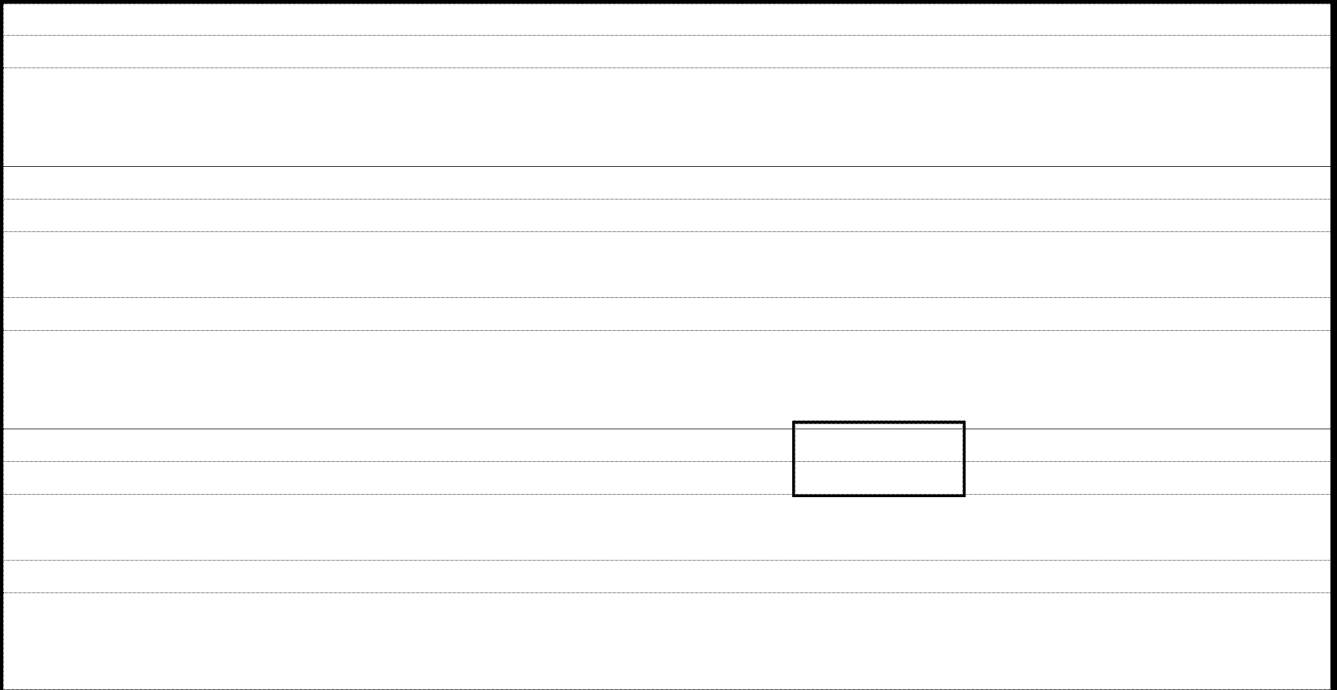
b6  
b7C  
b7E

# General Operational Guidelines





# General Operational Guidelines



A large white rectangular area with horizontal lines, serving as a template for text or a diagram.

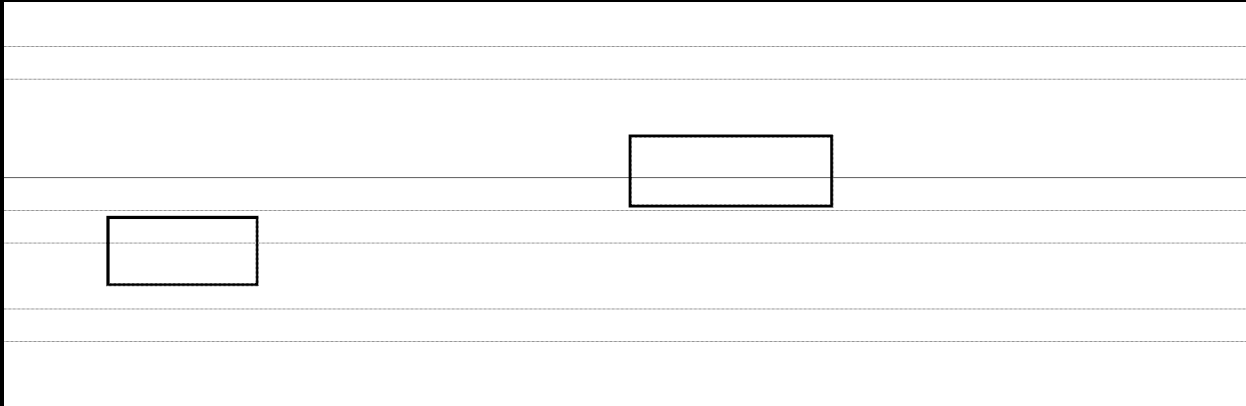


b7E

# General Operational Guidelines

b7E

# General Operational Guidelines



b6  
b7C

b7E

**Wake up.  
It's time to leave.**