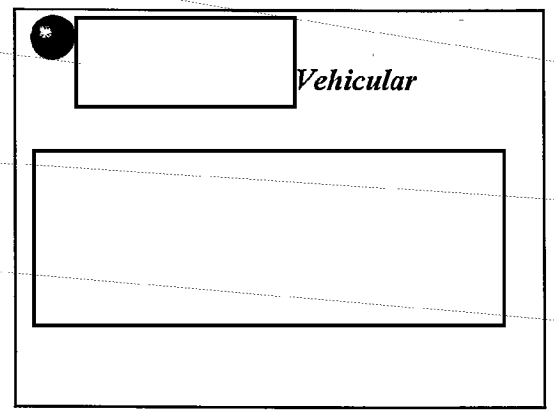
DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

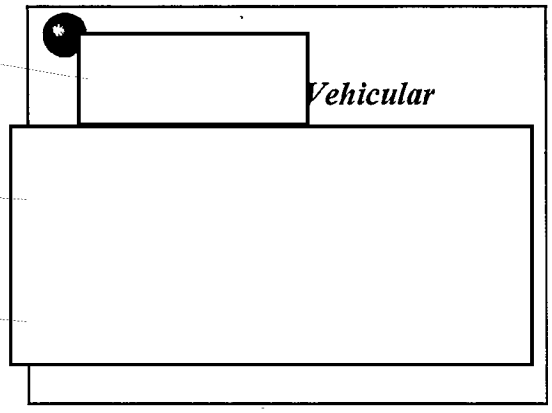
(S)

(S)



(S)

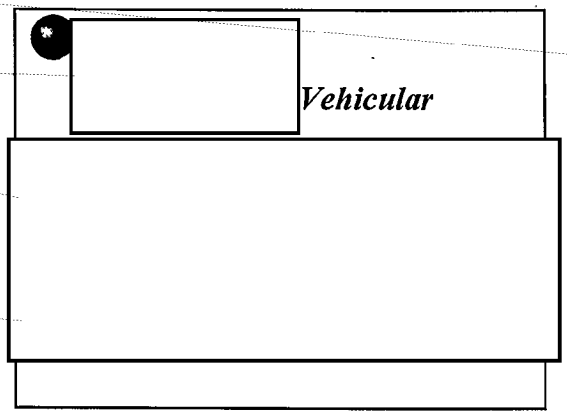
(S)



b1
b7E

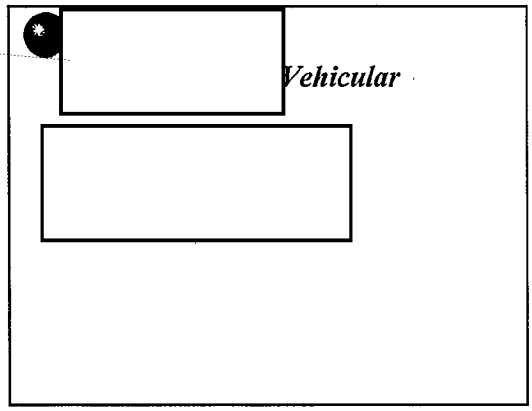
(S)

(S)



(S)

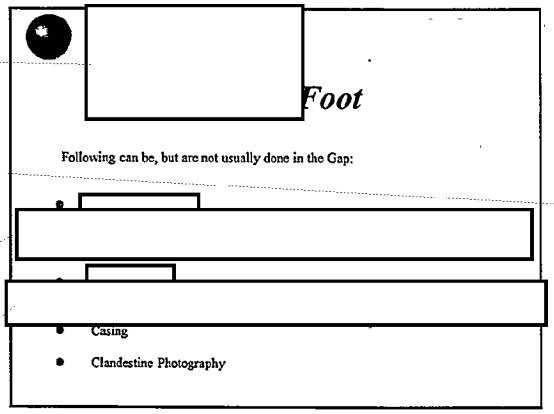
(S)



b1
b7E

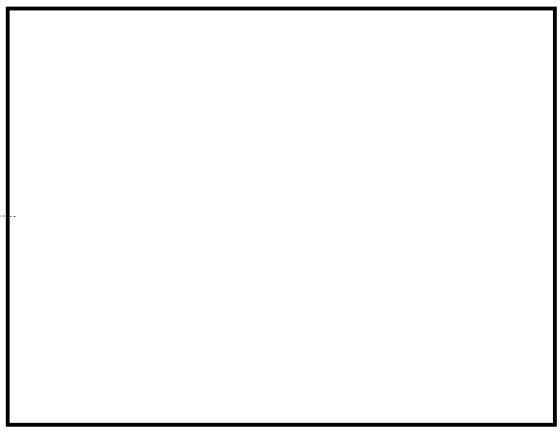
(S)

(S)



(S)

(S)



b1
b7E

5

(S)

(S)

Other Considerations

(S)

b1
b7E

(S)

(S)

Trends

b1
b7E

(S)

Trends

(S)

b1
b7E

(S)

(S)

b1
b7E

(S)

(S)

b1
b7E

(S)

Tactical Use of

b1
b7E

Strategic Use of [redacted]

Strategic CI Use of [redacted]

b1
b7E

[redacted] ***with a Source***

[redacted] ***with a Source***

b1
b7E

[redacted] ***with a source***

Review/Discussion

- Review the various forms of [redacted] seen today

b1
b7E

(S)

Fundamentals of [ ]

b7E

Questions?

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b7E

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-02

Classroom and Evening Practicals

September 7th - Monday - Travel Day - Meet at the Hotel at night (Time to be determined)

September 8th - Tuesday – Introduction and Area Familiarization

7:30 – 8:00 [redacted] students to get their Badges [redacted] **will ensure that they know where to go for the badges.** [redacted] **will ensure the** [redacted] **(around 7:00 AM) and ready to go and give the** [redacted] **info and badge to one of the** [redacted] **students to get everyone.** [redacted] **will get back to the CITC by 7:30 for the opening and intros, etc.**

b6 b7C b7E

8:00 – 8:25 Opening Comments, Intros, Orientation, and Objectives **(Give time to read what will be taught for the day – "** [redacted] **Considerations", "The Operational Environment", "Activities, Profiles, and** [redacted] **Analysis") -** [redacted]

8:25 – 8:30 **Break**

(S) 8:30 – 9:25 [redacted]

b1 b6 b7C b7E

9:25 – 9:30 **Break**

9:30 – 10:25 The Operational Environment – **Guest Speaker** [redacted]

[redacted] are given their cover, their legend and assignment.
Area Familiarization
Planning for your Assignment

b6 b7C b7E

10:25 – 10:30 **Break**

10:30 – 12:30 Activities, Profiles [redacted] Analysis – **Guest Speaker** [redacted]
Operational Site Selection
What to consider for [redacted]
[redacted]
What to consider for [redacted]
[redacted]
Reports (Have copies ready to hand out)

12:30 – 1:30 **Lunch**

1:30 – 6:30 Receive [redacted] and Field Work Assignment [redacted]
[redacted] regarding [redacted] **and**
[redacted]

b6 b7C b7E

6:30 - 7:00 **Dinner**

~~SECRET~~

(S)

September 9th - Wednesday [redacted]

b1 b6 b7C b7E

7:30 – 8:00 **(Time for [redacted] to read what will be taught for the day)**
[redacted] to ensure [redacted] by 7:20 and request students to read all material for this day

(S) [redacted]

8:00 – 8:15 Review of Area Familiarization, exercise, and objectives for the day – [redacted]
8:15 – 8:20 **Break**

8:20 – 10:00 (S) [redacted]

b1 b6 b7C b7E

10:00 – 10:05 **Break**

10:05 – 11:00 (S) [redacted]

b1 b6 b7C b7E

11:00 – 11:05 **Break**

11:05 – 12:00 (S) [redacted]

b1 b6 b7C b7E

- Review

12:00 – 1:00 **Lunch in Boardroom**

(S) 1:00 – 2:00 [redacted]

b1 b6 b7C b7E

2:00 – 2:30 Provide tasking for Field Work and Nightly Exercise Assignment – [redacted]
Lock up the Classroom and get back to the CITC.

(S) 2:30 - 6:00 Field Work Assignment: [redacted] site selection [redacted]

(S) [redacted]

b1 b6 b7C b7E

6:00 – 7:00 **Dinner**
7:00 – 10:00 Field Work Assignment

(S) **September 10th - Thursday -** [redacted]

b1
b6
b7C
b7E

7:30 – 8:00 **(Review all [redacted] reading material – prepare for test) – [redacted] to ensure the [redacted] by 7:20 and ready to go. Ensure the [redacted] understand what they have read thus far.**

8:00 – 8:15 Review of exercise/ **test/** and objectives for the day: Op Site Selection with [redacted] Techniques / Critique – [redacted]

8:15 – 8:20 **Break**

b6
b7C
b7E

8:20 – 9:30 Introduction to [redacted] (Pick out video that they have not seen before) – [redacted]

9:30 – 9:35 **Break**

9:35 – 10:30 Introduction to [redacted]

10:30 – 10:35 **Break**

10:35 – 11:30 Introduction to [redacted]

11:30 – 12:00 Wrap Up & Briefing on Field Work Assignment

[redacted]

12:00 – 1:00 Lunch in Board Room

(S) 1:00 – 3:00 [redacted]

- Techniques, strategies, operations, and [redacted]
- Lesson's Learned

b1
b6
b7C
b7E

[redacted] **to stay with [redacted] during this last presentation and provide transportation for him back to his Hotel)**

3:00 – 6:00 Field Work Assignment

6:00 – 7:00 **Dinner**

7:00 – Done Field Work Assignment

(S) **September 11th - Friday -** [redacted]

7:30 – 8:00 **(Give time to [redacted] to read what will be taught for the day, review all reading material, prepare for test, review operational sites) – [redacted] to ensure the [redacted] by 7:20 and ready to go. Ensure the [redacted] understand what they have read thus far.**

8:00 – 8:15 Review of exercise, test, and objectives for the day / Critique – [redacted]

(S) 8:15 – 9:25 [redacted]

9:25 – 9:30 Break

(S) 9:30 – 10:25 [redacted]

10:25 – 10:30 **Break**

(S) 10:30 – 11:25 [redacted]

11:25 – 11:30 **Break**

(S) 11:30 – 12:30 [redacted]

12:30 – 1:30 **Lunch in board Room**

(S) 1:30 – 2:15 [redacted]

2:15 – 2:30 **Break**

2:30 - 6:00 Practice [redacted]

6:00 – 7:00 Dinner

7:00 – Done TRAVEL TO [redacted] CHECK-IN

b1
b6
b7C
b7E

b1
b6
b7C
b7E

b1
b6
b7C
b7E

b6
b7C
b7E

September 12th Saturday

8:00 – 8:30 Meet in the Hotel Conference Room - Critique for Friday –

9:00 – 12:00 Finish the Field Work Assignments and Op Act Practice preparation for following week's practical:

(S)

(All are to do the Op Sites, casing, and runs ahead of next week)

b1
b6
b7C
b7E

12:00 – 1:00 **Lunch**

(S)

1:00 – 6:00 Area Familiarization

b1
b7E

6:00 – 7:00 Dinner

7:00 – 8:00 Meeting in Hotel Conference Room – Wrap up and prep for next week.

September 13th Sunday

Day of Rest

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-02

Classroom and Evening Practicals

b7E

September 7th - Monday - Travel Day - Meet at the Hotel at night (Time to be determined)

September 8th - Tuesday – Introduction and Area Familiarization

7:30 – 8:00 [redacted] students to get their Badges

8:00 – 8:25 Opening Comments, Intros, Orientation, and Objectives **(Give time to read what will be taught for the day – [redacted] Considerations", "The Operational Environment", "Activities, Profiles, and [redacted] nalysis")** b7E

8:25 – 8:30 **Break**

(S) 8:30 – 9:25 [redacted] b1 b7E

9:25 – 9:30 **Break**

9:30 – 10:25 The Operational Environment - [redacted] are given [redacted] b7E
Area Familiarization
Planning for your Assignment

10:25 – 10:30 **Break**

10:30 – 12:30 Activities, Profiles [redacted] Analysis [redacted]
What to consider fo [redacted] b7E
What to consider fo [redacted]
[redacted] (Have copies ready to hand out)

12:30 – 1:30 **Lunch**

1:30 – 6:30 Field Work Assignment - [redacted]
Students will be required to answer questions regarding [redacted] b7E
[redacted] to help facilitate area familiarization.

6:30 - 7:00 **Dinner**

~~SECRET~~

(S) **September 9th - Wednesday** [redacted]

7:30 – 8:00 **(Time for [redacted] to read what will be taught for the day)**

8:00 – 8:15 Review of Area Familiarization, exercise, and objectives for the day - b1 b7E

8:15 – 8:20 **Break**

8:20 – 10:00 (S) [redacted]

10:00 – 10:05 **Break**

10:05 – 11:00 (S) [redacted] b1 b7E

11:00 – 11:05 **Break**

11:05 – 12:00 (S) [redacted] b1 b7E

- Review

12:00 – 1:00 **Lunch in Boardroom**

1:00 – 2:00 (S) [redacted] b1 b7E

2:00 – 2:30 Provide tasking for Field Work and Nightly Exercise Assignment

2:30 - 6:00 (S) Field Work Assignment: [redacted] b1 b7E

6:00 – 7:00 (S) **Dinner**

7:00 – Done Field Work Assignment

April 10th - Thursday - [redacted] b1 b7E

(S) 7:30 – 8:00 **(Review all [redacted] reading material – prepare for test) -**

8:00 – 8:15 Review of exercise/ **test/** and objectives for the day: Op Site Selection with [redacted] Techniques / Critique –

8:15 – 8:20 **Break**

8:20 – 9:30 Introduction to [redacted] (Pick out video that they have not seen before) –

9:30 – 9:35 **Break**

9:35 – 10:30 Introduction to [redacted] – b7E

10:30 – 10:35 **Break**

10:35 – 11:30 Introduction to [redacted] –

11:30 – 12:00 Wrap Up & Briefing on Field Work Assignment

[redacted]

12:00 – 1:00 Lunch in Board Room

(S) 1:00 – 3:00 [redacted] b1 b6 b7C b7E

- Techniques, strategies, operations, and [redacted] recruiting"
- Lesson's Learned

[redacted] to reiterate the brief to the [redacted] regarding what they need to do and lock up the [redacted]

3:00 – 6:00 Field Work Assignment

6:00 – 7:00 **Dinner**

7:00 – Done Field Work Assignment

(S) **September 11th - Friday -** [redacted]

7:30 – 8:00 **(Give time to [redacted] to read what will be taught for the day, review all reading material, prepare for test, review [redacted]**

8:00 – 8:15 Review of exercise, **test**, and objectives for the day / Critique –

8:15 – 9:25 (S) [redacted]

9:25 – 9:30 Break

9:30 – 10:25 (S) [redacted]

10:25 – 10:30 **Break**

10:30 – 11:25 (S) [redacted]

11:25 – 11:30 **Break**

11:30 – 12:30 (S) [redacted]

12:30 – 1:30 **Lunch in board Room**

1:30 – 2:15 (S) [redacted]

2:15 – 2:30 **Break**

2:30 - 6:00 Practice [redacted]

6:00 – 7:00 Dinner

7:00 – Done TRAVEL TO [redacted] CHECK-IN

b1
b7E

b7E

b1
b7E

b1
b7E

b1
b7E

b7E

April 18th Saturday

8:00 – 8:30 Meet in the Hotel Conference Room - Critique for Friday –

9:00 – 12:00 Finish the Field Work Assignments and Op Act Practice preparation for following week's practical

(S) [redacted] b1 b7E

(All [redacted] are to do the [redacted] Op Sites, [redacted] head of next week)

12:00 – 1:00 **Lunch**

1:00 – 6:00 Area Familiarization.

(S) [redacted] b1 b7E

6:00 – 7:00 Dinner

7:00 – 8:00 Meeting in Hotel Conference Room – Wrap up and prep for next week.

April 19th Sunday
Day of Rest

The rest of schedule follows the SOC schedule as the [redacted] operate against the 4 SOC Teams. b7E

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-02

Classroom and Evening Practicals

September 7th - Monday - Travel Day - Meet at the Hotel at night (Time to be determined)

September 8th - Tuesday – Introduction and Area Familiarization

7:30 – 8:00 [redacted] students to get their Badges

8:00 – 8:25 Opening Comments, Intros, Orientation, and Objectives **Read** [redacted] **Considerations", "The Operational Environment", "Activities, Profiles, and** [redacted] **Analysis"** – [redacted]

(S) 8:25 – 8:30 **Break**

8:30 – 9:25 [redacted] **with**

(S) **Guest Speakers** [redacted] Cover Considerations [redacted]

9:25 – 9:30 **Break**

9:30 – 10:25 The Operational Environment – [redacted] **with Guest Speakers** [redacted] **and** [redacted] are given [redacted]
Area Familiarization and Planning for your Assignment

10:25 – 10:30 **Break**

10:30 – 12:30 Activities, Profiles [redacted] Analysis – [redacted] **with Guest Speakers** [redacted]
Operational Site Selection
What to consider for [redacted]
What to consider for [redacted]
Operational Site Reports/ Surveys

12:30 – 1:30 **Lunch**

1:30 – 6:30 Receive [redacted] Field Work Assignment – [redacted] regarding [redacted]

6:30 - 7:00 **Dinner**

~~SECRET~~

(S) **September 9th - Wednesday –** [redacted]

b1
b6
b7C
b7E

(S) 7:30 – 8:00 [redacted]

8:00 – 8:15 Review of Area Familiarization, exercise, and objectives for the day – [redacted]

8:15 – 8:20 **Break**

8:20 – 10:00

(S) [redacted]

b1
b7E

10:00 – 10:05 **Break**

10:05 – 11:00

(S) [redacted]

b1
b7E

11:00 – 11:05 **Break**

11:05 – 12:00

(S) [redacted]

b1
b7E

- Review

12:00 – 1:00 **Lunch in Boardroom**

(S) 1:00 – 2:00 [redacted]

2:00 – 2:30 Provide tasking for Field Work and Nightly Exercise Assignment – [redacted]

(S) 2:30 - 6:00 Field Work Assignment: area fam for quads 2 and 4, site selection [redacted]

b1
b6
b7C
b7E

(S) [redacted]

6:00 – 7:00 **Dinner**
7:00 – 10:00 Field Work Assignment

September 10th - Thursday - [redacted]

(S)

7:30 – 8:00 **Review al** [redacted] **reading material – prepare for test**

8:00 – 8:15 Review of exercise/ **test**/ and objectives for the day: Op [redacted] with [redacted] Techniques / Critique – [redacted]

8:15 – 8:20 **Break**

8:20 – 9:30 Introduction to [redacted]

9:30 – 9:35 **Break**

9:35 – 10:30 Introduction to [redacted]

10:30 – 10:35 **Break**

10:35 – 11:30 Introduction to [redacted]

11:30 – 12:00 Wrap Up & Briefing on Field Work Assignment - [redacted]

12:00 – 1:00 Lunch in Board Room

(S)

1:00 – 3:00 [redacted]

- Techniques, strategies, operations, and [redacted]
- Lesson's Learned

3:00 – 6:00 Field Work Assignment - [redacted]

6:00 – 7:00 **Dinner**

7:00 – Done Field Work Assignment

b1
b6
b7C
b7E

b1
b6
b7C
b7E

~~SECRET~~

(S) [redacted]

September 11th - Friday - [redacted]

(S) 7:30 – 8:00 **Review All** [redacted] **Info and reading material – Prep for test.**

8:00 – 8:15 Review of exercise, **test**, and objectives for the day / Critique – [redacted]

8:15 – 9:25 [redacted]

(S)

9:25 – 9:30 Break

9:30 – 10:25 [redacted]

(S)

10:25 – 10:30 **Break**

10:30 – 11:25 [redacted]

(S)

11:25 – 11:30 **Break**

11:30 – 12:30 [redacted]

(S)

12:30 – 1:30 **Lunch in board Room**

1:30 – 2:15 [redacted]

(S) 2:15 – 2:30 **Break**

2:30 - 6:00 Car Escape [redacted] –

[redacted]

6:00 – 7:00 Dinner

7:00 – Done

b1
b6
b7C
b7E

b1
b7E

b1
b7E

b6
b7C
b7E

~~SECRET~~

September 12th Saturday

8:00 – 8:30 Meet in the Hotel Conference Room - Critique for Friday –

9:00 – 12:00 Finish the Field Work Assignments

12:00 – 1:00 **Lunch**

(S) 1:00 – 6:00 Area Familiarization

6:00 – 7:00 Dinner

b1
b7E

September 13th Sunday

Day of Rest **- Get some Sleep. You will need it.**

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET/NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)

(S)

(S)

b1
b7E

(S)

b1
b7E

(S)

~~SECRET/NOFORN~~

Prepared by SSA

b6
b7C

(S)

b1
b7E

IV. OPERATIONAL ACT EXAMPLES

(S)

(S) 1)

b1
b7E

(S) 2)

(S) 3)

(S) 4)

b1
b7E

(S)

(S) 1)

(S) 2)

(S) 3)

b1
b7E

Prepared by SSA

b6
b7C

(S) 4)

(S) 5)

(S) 6)

(S) 7)

(S) 8)

(S) 9)

b1
b7E

(S)

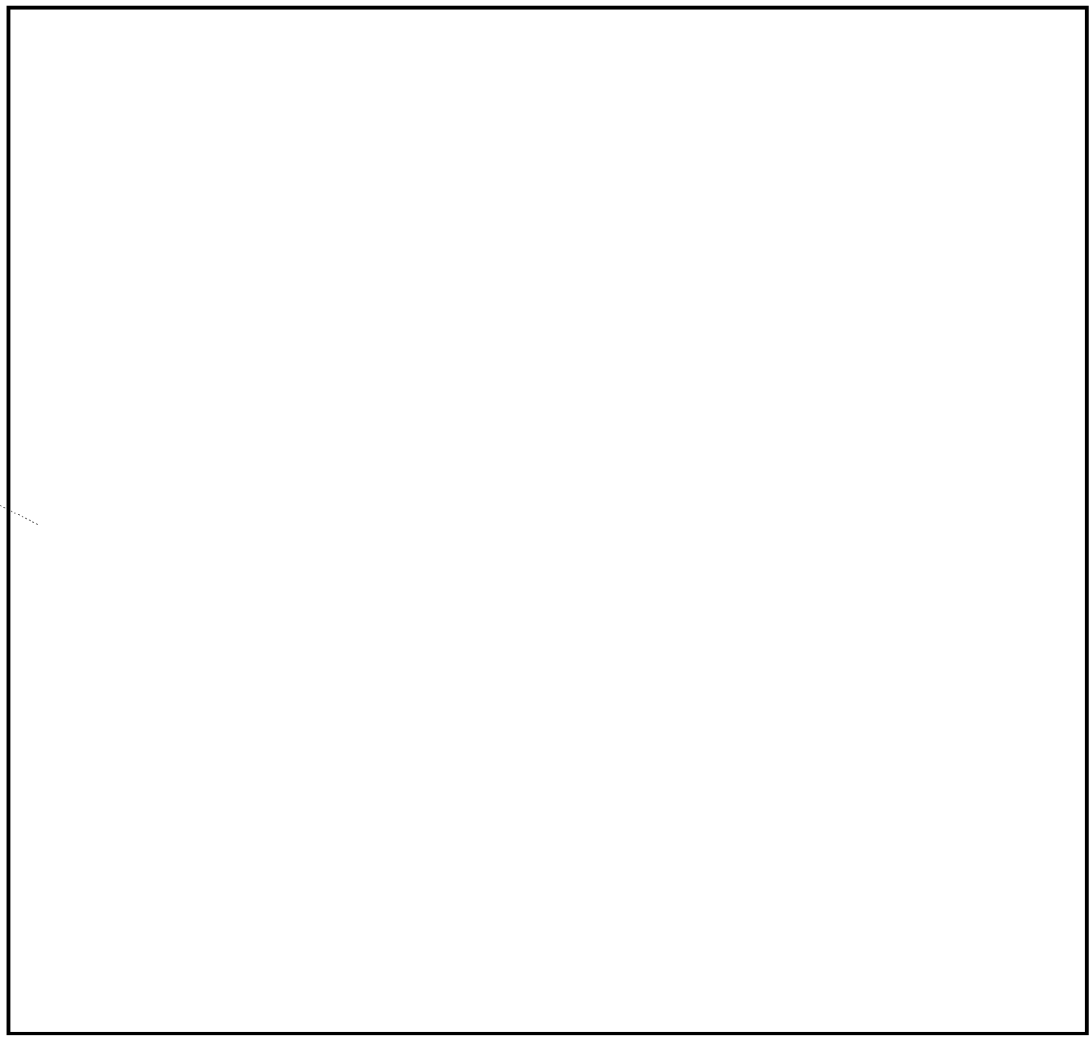
b1
b7E

(S) 3)

b1
b7E

Prepared by SSA

b6
b7C



(S)

b1
b7E

V. Final Thoughts



(S)

b1
b7E

Prepared by SSA

b6
b7C

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-01

Practical Application Week

b1
b7E

Cover For Status

(S) [redacted]

Each student will conduct a [redacted] followed by an [redacted] b7E

[redacted]

September 14 - 18

	Day Shift (9 am – 1 pm)	Night Shift (5 pm – 9 pm)
	8- 8:15: Brief	4 – 4:15 Brief
(S)	8:15 – 8:30 [redacted]	4:15 – 4:30 [redacted]
	8:30 – 9:00	4:30 – 5:00
	9 – 1 Shift	5 – 9 Shift
(S)	1 – 1:30 Back to CP	9 – 9:30 Back to CP
	1:30 – 3 Debrief / determine status	9:30 - 11 Debrief / determine status

b1
b7E

M	Kick-off points	Kick-off points
(S)	[redacted]	

b1
b7E

T	Kick-off points	Kick-off points
(S)	[redacted]	

b1
b7E

W	Kick-off points	Kick-off points
(S)	[redacted]	

b1
b7E

~~SECRET~~

Th Kick-off points Kick-off points

(S) [redacted] b1 b7E

(S) F [redacted]

9:00 am kick off [redacted]
9:30 am kick off
1:00 End of the practical

(S) [redacted] b1 b7E

2:00 - 3:00
3:00 - 5:00 Clean up/check in gear
5:00 - 6:00 Class Debriefing –Class Video in Hotel Conference Room
6:00 - ???? Class Party and dinner at [redacted]

Saturday September 19 – Travel day - Go home and get some well earned Sleep.

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-01

b7E

Practical Application Week

Cover For Status

(S) [redacted]

b1
b7E

(S) [redacted]

	Day Shift (9 am – 1 pm)	Night Shift (5 pm – 9 pm)
	8- 8:15: Brief	4 – 4:15 Brief
	8:15 – 8:30	4:15 – 4:30
(S)	8:30 – 9:00 [redacted]	4:30 – 5:00 [redacted]
	9 – 1 Shift	5 – 9 Shift
	1 – 1:30 Back to CP	9 – 9:30 Back to CP
(S)	1:30 – 3 Debrief / determine status	9:30 - 10 Debrief / determine status
M	1,2,5,6 Kick-off points	3,4,7,8 Kick-off points

(S) [redacted]

b1
b7E

T	3,4,7,8 Kick-off points	1,2,5,6 Kick-off points

(S) [redacted]

b1
b7E

W	1,2,5,6 Kick-off points	3,4,7,8 Kick-off points

(S) [redacted]

b1
b7E

~~SECRET~~

Th 3,4,7,8 Kick-off points 1,2,5,6 Kick-off points

(S) [redacted] b1 b7E

(S) F [redacted]

9:00 am kick off [redacted]
9:30 am kick off
1:00 End of the practical

b1 b7E

2:00 - 3:00 [redacted]
3:00 - 5:00 Clean up/check in gear
(S) 5:00 - 6:00 Class Debriefing –Class Video in Hotel Conference Room
6:00 - 8:00 Class Party and dinner at [redacted]

Sdnt	Monday (14th)	Tuesday (15st)	Wednesday (16nd)	Thursday (17rd)	Friday (18th)
1					
2					
3					
4					
5					
6					
7					
8					

b1 b7E

(S)

Saturday – Travel day - go get some Sleep.

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-01

b7E

Practical Application Week

[redacted] Students (Official: 1, 2, 3, 4, Comm: 5, 6, 7, 8)

Cover For Action

(S) [redacted]

(S) [redacted]

b1
b7E

	Day Shift (9 am – 1 pm)	Night Shift (5 pm – 9 pm)
M	1,2,5,6 Kick-off points	3,4,7,8 Kick-off points

(S) [redacted]

(S) [redacted]

b1
b7E

[redacted]

[redacted]

T	3,4,7,8 Kick-off points	1,2,5,6 Kick-off points

b1
b7E

(S) [redacted]

(S) [redacted]

~~SECRET~~

(S)

(S) W 1,2,5,6 Kick-off points 3,4,7,8 Kick-off points

(S)

(S)

b1
b6
b7C
b7E

1, 3, 6, 8 will

Th 3,4,7,8 Kick-off points 1,2,5,6 Kick-off points

(S)

(S)

(S)

(S)

b1
b6
b7C
b7E

3, 4, 5, 7,8 will do a

1,2

(S)

(S) F All Play (Will be doing

9:00 am kick of

9:30 am kick of

b1
b7E

(S) 2:00 - 3:00

3:00 - 5:00 Clean up/check in gear

6:00 - 8:00 Video/Class Party in hotel conf room, dinner

(S)

Sdnt	Monday (20th)	Tuesday (21st)	Wednesday (22nd)	Thursday (23rd)	Friday (24th)
1					
2					
3				Meet	
4			Meeting	Meet	
5			Meeting	Meet	
6		Meeting		Meet	
7					
8					

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

b1
b6
b7C
b7E

Will need a total of four (4) role players for each day.

(S)

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE [redacted] OPERATIONS COURSE #09-01 b7E

Classroom and Evening Practicals
Instructor Schedule

April 13th - Monday - Travel Day

April 14th - Tuesday – Introduction and Area Familiarization

8:00 – 8:25 Opening Comments, Introductions, Orientation, and Course Objectives - [redacted] b1 b6 b7C b7E

8:25 – 8:30 **Break**

(S) 8:30 – 9:25 [redacted]

- The Adversary

9:25 – 9:30 **Break**

9:30 – 10:25 Area Familiarization, [redacted]

- Planning for your Assignment

10:25 – 10:30 **Break**

10:30 – 12:00 Area Familiarization [redacted] Continued) - [redacted] b1 b6 b7C b7E

(S) - [redacted]

- What to consider for [redacted] (CPU [redacted] Meetings)
- What to consider for [redacted]

12:00 – 1:00 **Lunch**

1:00 – 6:00 [redacted] Exercise - [redacted]

- Students will be required to answer [redacted] questions regarding [redacted] to help facilitate area familiarization. b7E
- Students will be required to [redacted]

6:00 - 7:00 **Dinner**

~~SECRET~~

(S)

April 15th - Wednesday [redacted]

b1
b6
b7C
b7E

8:00 – 9:00 Review of [redacted] exercise, and objectives for the day - [redacted]

9:00 – 9:10 **Break**

9:10 – 10:00 [redacted]

(S)

b1
b6
b7C
b7E

10:00 – 10:10 **Break**

10:10 – 11:00 [redacted]

(S)

(S)

11:00 – 11:10 **Break**

11:10 – 12:15 [redacted]

12:15 – 1:15 **Lunch in Boardroom**

b1
b6
b7C
b7E

1:15 – 2:15 [redacted]

(S)

2:15 – 6:00

6:00 – 7:00 **Dinner**

7:00 – Done Complete Exercise Requirements

April 16th - Thursday - [redacted]

b6
b7C
b7E

8:00 – 8:30 Review of exercise and objectives for the day / Critique - [redacted]

8:30 – 9:45 Introduction to [redacted] - **Guest Instructor**

- Terminology
- Trends

(S) [redacted]

b1
b7E

9:45 – 9:50 **Break**

9:50 – 10:50 Introduction to [redacted] - **Guest Instructor**

(S) [redacted]

(S) [redacted]

(S) [redacted]

b1
b7E

10:50 – 11:00 **Break**

11:00 – 12:00 [redacted] - **Guest Instructor**

- Final comments, review

b7E

12:00 – 1:00 Lunch

1:00 – 2:00 [redacted]

- [redacted]

b6
b7C
b7E

2:00 – 2:05 Break

b1
b6
b7C
b7E

(S) 2:05 – 4:00 [redacted]

- Techniques, strategies, operations, and [redacted]
- Lesson's Learned

4:00 – 4:30 Brief on Practical Exercise - [redacted]

- [redacted]
- Operational Activities
  - [redacted] Two

4:30 – 6:00 Field Work

- [redacted]

(S) [redacted]

b1
b7E

6:00 – 7:00 **Dinner**

7:00 – Done Field Work

(S)

April 17th - Friday - [redacted]

8:00 – 8:30 Review of exercise and objectives for the day / Critique - [redacted]

(S) 8:30 – 9:25 [redacted]

b1
b6
b7C
b7E

9:25 – 9:30 Break

9:30 – 10:25 (S) [redacted]

10:25 – 10:30 **Break**

10:30 – 11:25 Getting a Second Meeting - [redacted]

(S) [redacted]

(S) [redacted]

b1
b6
b7C
b7E

11:25 – 11:30 **Break**

11:30 – 12:30 (S) [redacted]

b1
b6
b7C
b7E

12:30 – 1:30 **Lunch**

(S) 1:30 – 2:15 [redacted] Continued - [redacted]

2:15 – 2:30 **Break**

2:30 - 6:00 Practice of [redacted] – Guest Instructors

6:00 – 7:00 Dinner

b7E

7:00 – Done TRAVEL TO [redacted] CHECK-IN

April 18th Saturday

(S)

9:00 – 12:00 Observation [redacted]

- 9:00 – 10:30 Group One
- 10:30 – 12:00 Group Two

b1
b7E

12:00 – 1:00 **Lunch**

1:00 – Done Area Familiarization [redacted] Preparation for Following Week's Practical

- All [redacted] must be completed by close of business and reviewed by instructor.

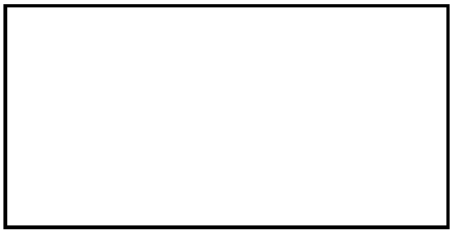
b7E

April 19th Sunday

Day of Rest

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-13-2012 BY 65179/DMH/BAW/STP/bls

Now Hit the Street !! (3)



Now Hit the Street !! (4)



b7E

Return to office (5)



Getting there is half the fun, right?? "ROAD TRIP!!!!"



b7E

Questions??

Good Luck and Have Fun!!

DATE: 01-06-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-06-2037

~~SECRET~~ ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE 7/13/2011

[redacted]:
OBSERVATION SKILLS

OBSERVATION: PRINCIPLES

OBSERVATION:
- Act of seeing or fixing the mind upon something for the purpose of recognizing and retaining some fact or occurrence
- Requires conscious and continuous effort

Attention:
- Awareness of surroundings
- Voluntary attention to the activity they are undertaking
- Involuntary attention if it does not fit within an individual's frame of reference – something/someone that draws attention

Perception:
- Everyone perceives his/her surroundings uniquely
- Based on background, culture, experiences
- Overcome preconceived ideas through training and concentration

Retention:
- Capture what you see

b7E

(S)
(S)
(S)

OBSERVATION: PURPOSE

[redacted]

- Agent safety
- [redacted]
- Personal security
- Briefing and debriefing
- [redacted]
- Assessment

b1
b7E

(S)
(S)

OBSERVATION: GOALS

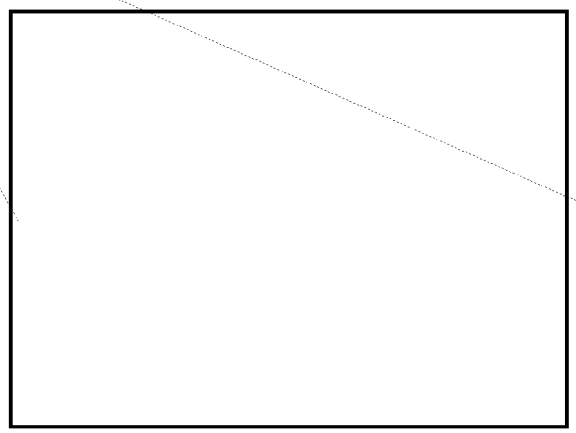
[redacted]

b1
b7E

~~SECRET~~
ACLURM031991
FBI031511

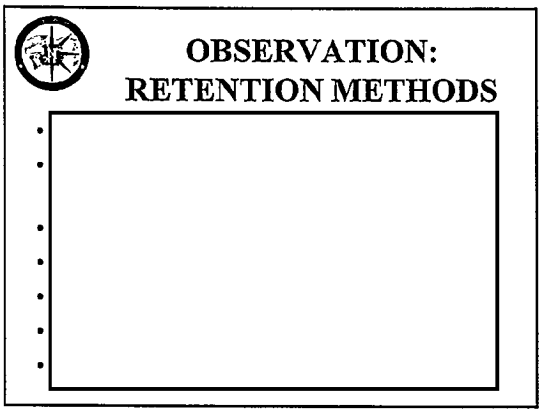
(S)

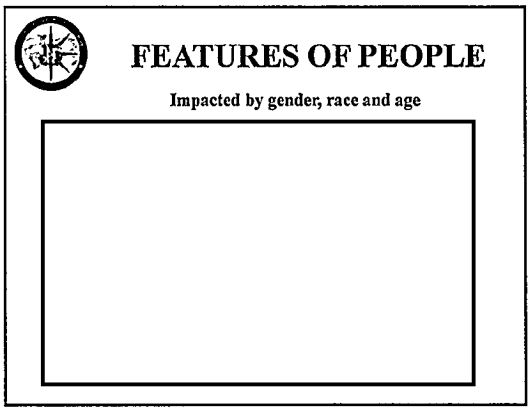
(S)



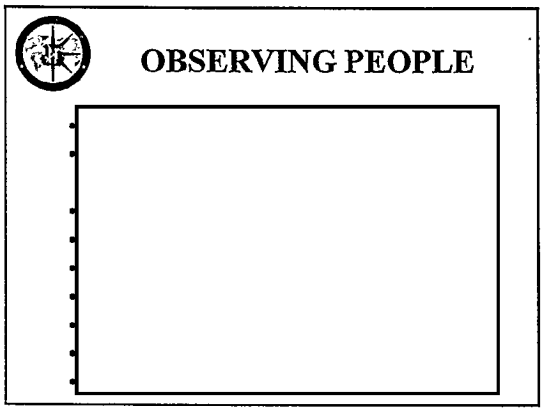


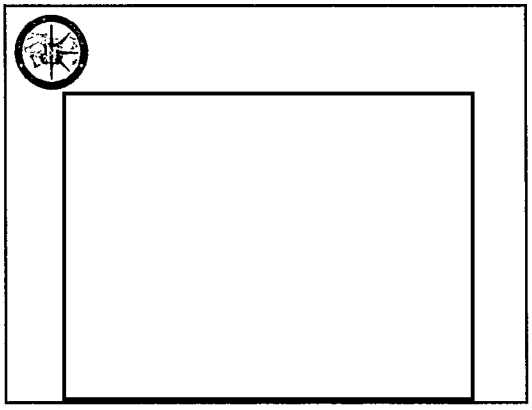
b1
b7E



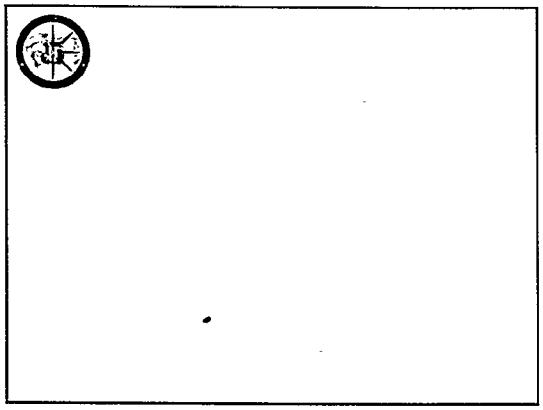


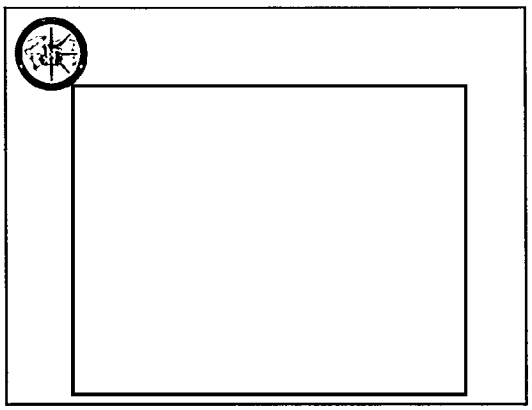
b7E



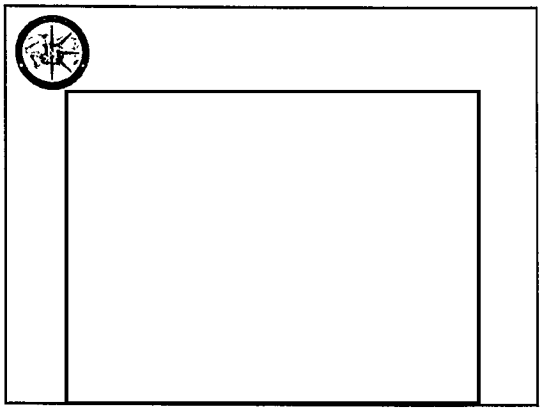


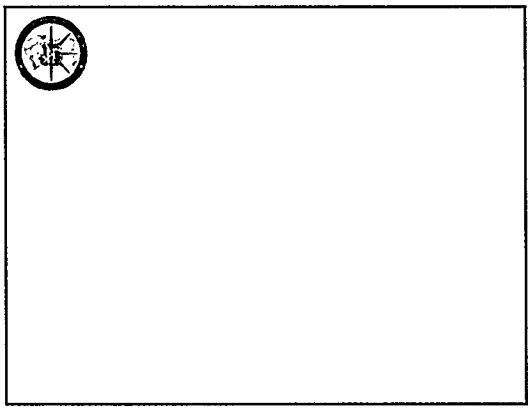
b6
b7C
b7E



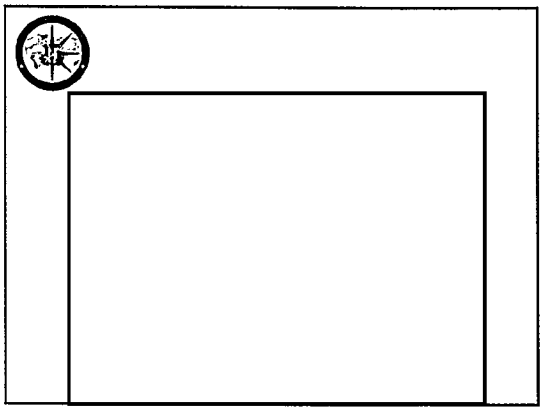


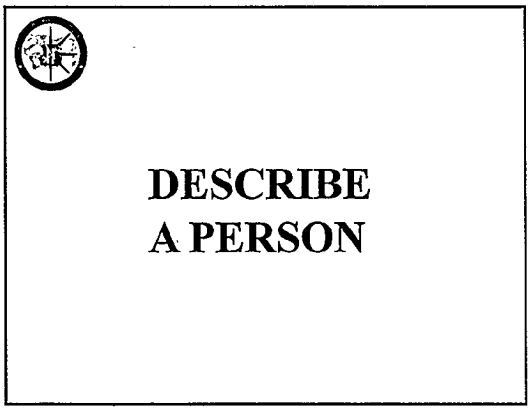
b6
b7C
b7E



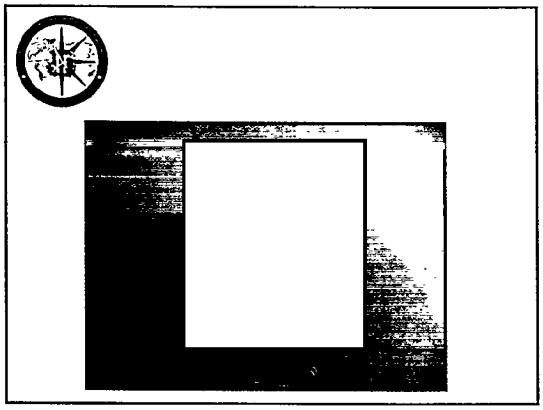


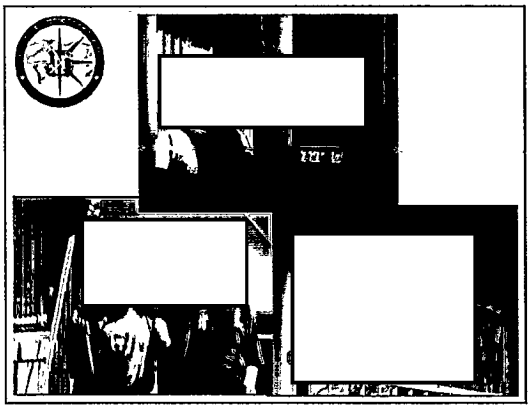
b6
b7C
b7E



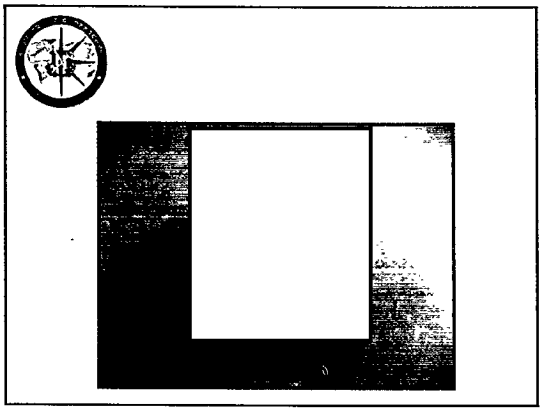


b6
b7C
b7E





b6
b7C



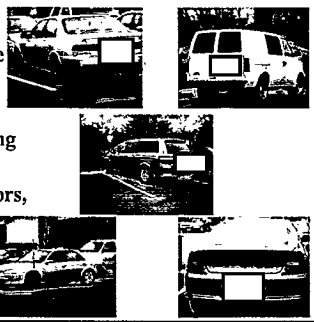
FEATURES OF CARS

- Plate number
- Color, make, model
- Signatures: scratches, hubcaps, dents, license plate covers, decals
- Profile of individuals in vehicle

b6
b7C

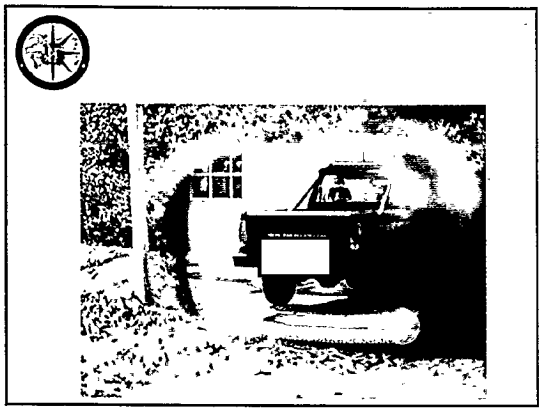
OBSERVING CARS

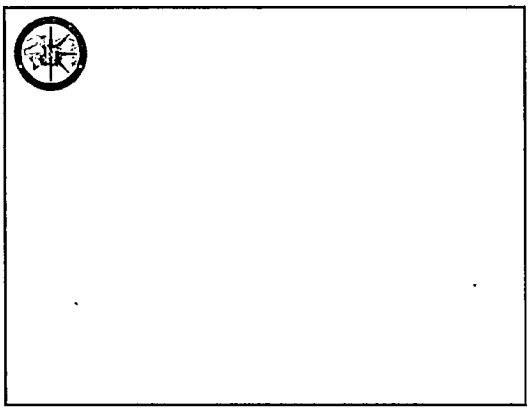
- Key in on the plate
- Know your makes and logos
- Look for identifying marks
- Avoid pitfalls (colors, common types)
- Taxis



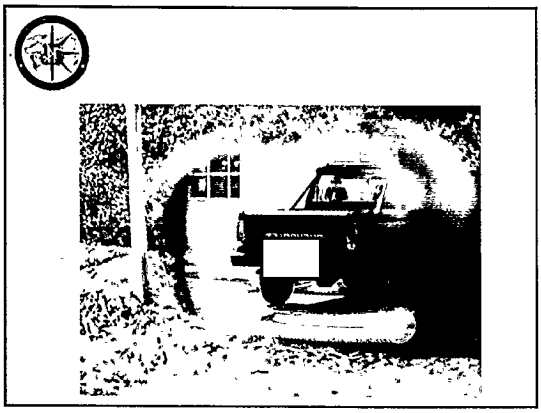
OBSERVE A CAR

b6
b7C



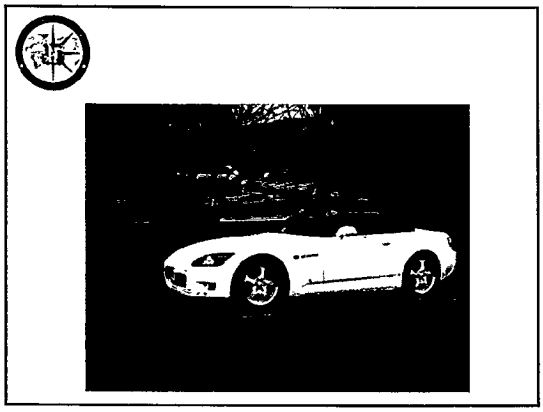


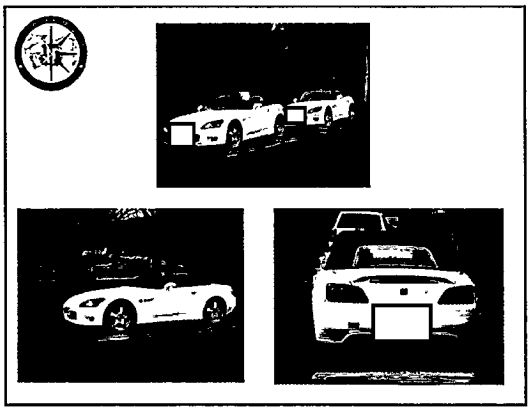
b6
b7C



DESCRIBE A CAR

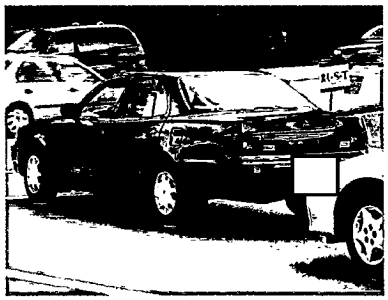
b6
b7C





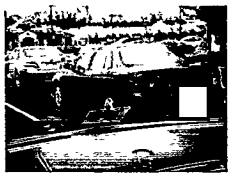
b6
b7C

DESCRIBE A CAR



b6
b7C

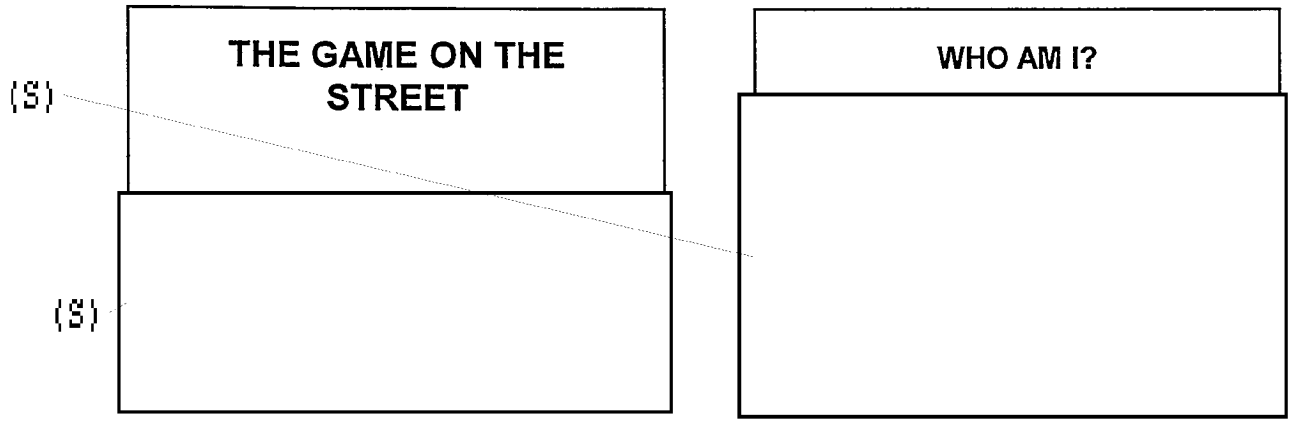




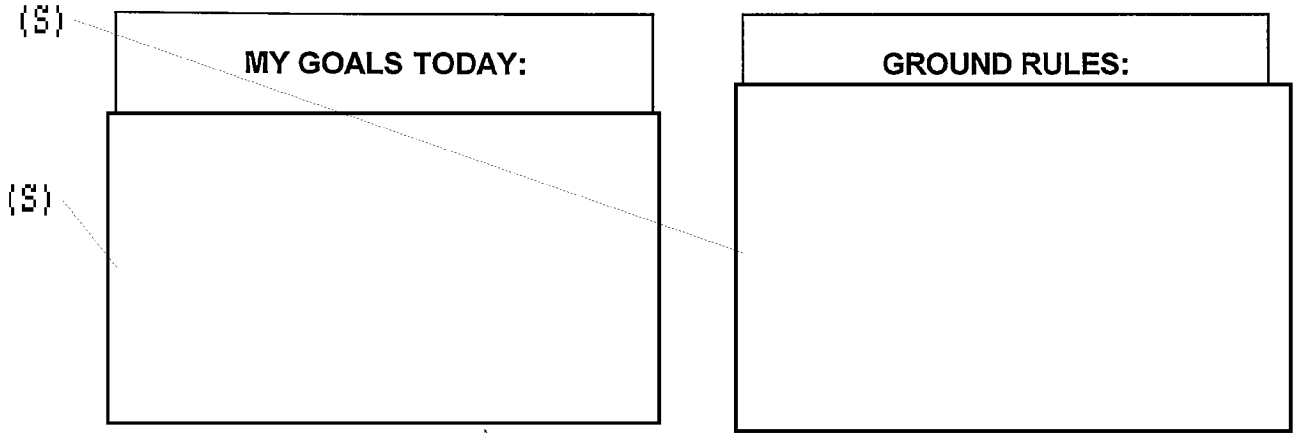
TWO TRUTHS

- Observations skills, coupled with area knowledge, can save your life in high threat situations
- Under stress you will lose the ability to make valid observations unless you practice

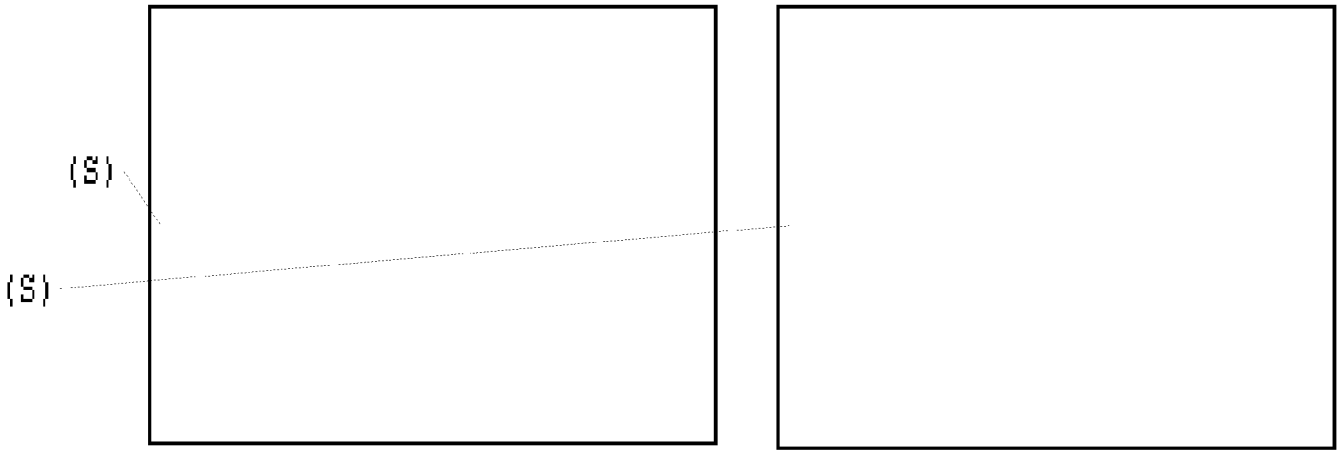
b6
b7C



b1
b7E



b1
b7E



b1
b7E

(S)

(S)

b1
b7E

(S)

(S)

b1
b7E

(S)

(S)

LET'S LOOK AT SOME

b1
b7E

(S)

(S)

I MIGHT DO THIS:

b1
b7E

(S)

(S)

I MIGHT TRY THIS:

b1
b7E

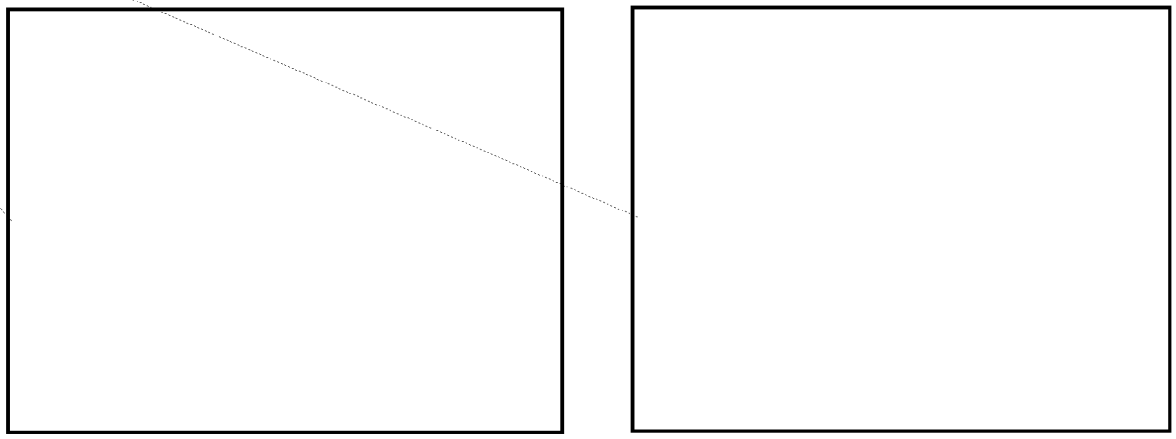
(S)

(S)

b1
b7E

(S)

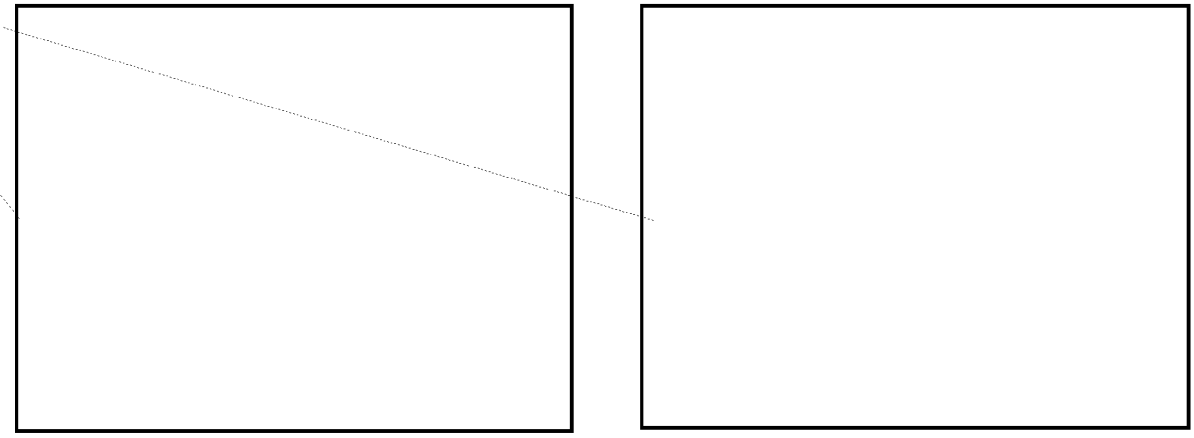
(S)



b1
b7E

(S)

(S)



b1
b7E

QUESTIONS?

COMMENTS?

(S)

b1
b7E

(S)

(S)

INTRODUCTION TO [redacted]

"What you're seeing isn't necessarily what's happening."

[redacted]

b1
b7E

(S)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

[redacted]

[redacted]

b1
b7E

(S)

(S)

(S)

(S)

(S)

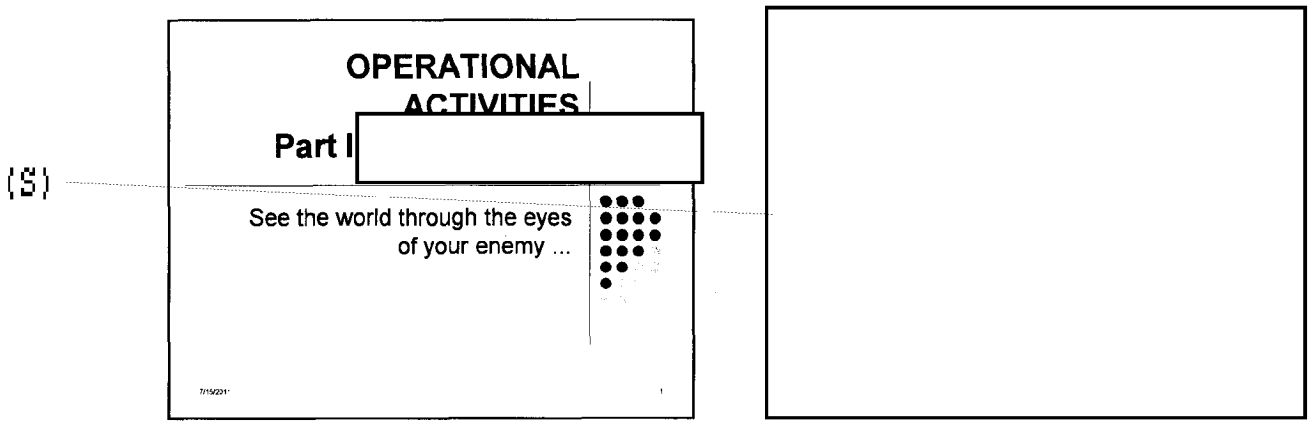
[redacted] **- Miscellaneous**

[redacted]

b1
b7E

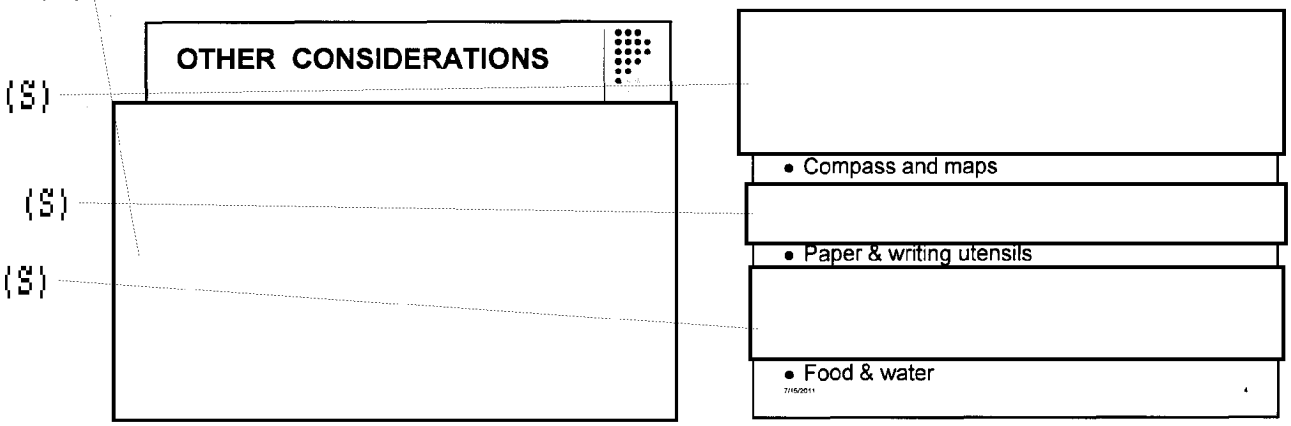
~~SECRET~~

copy



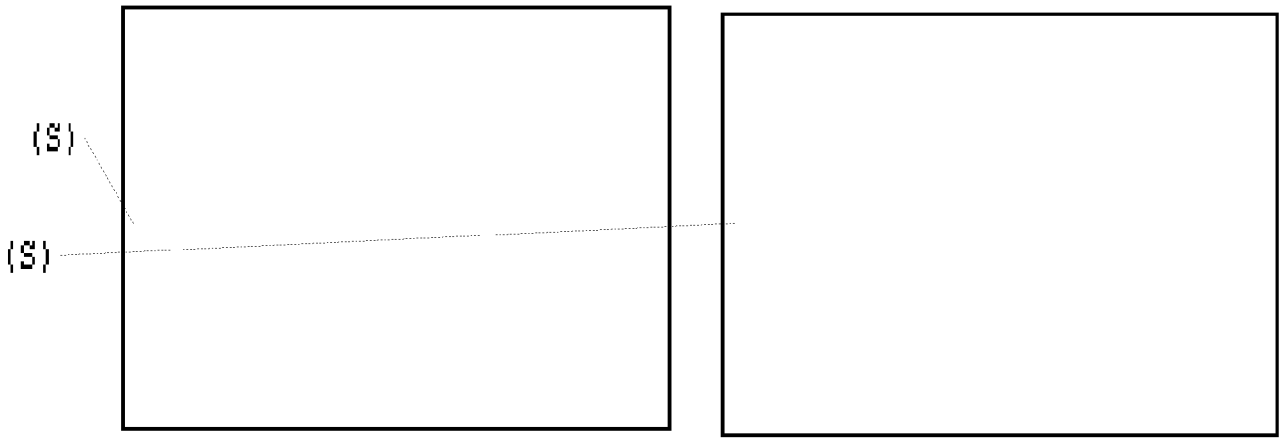
(S)

b1
b7E



(S)
(S)
(S)
(S)

b1
b7E



(S)
(S)

b1
b7E

Fundamentals of [redacted]

(S) [redacted] *is universal.*

Tools of the [redacted]

Fundamentals of [redacted]
Lesson Overview

This course will introduce you to the fundamentals of [redacted]

b1
b7E

[redacted] *Objectives*

At the end of this course students will:

- Be able to detect various forms of [redacted]
- Describe various forms and levels of [redacted]
- Use [redacted] in an operational training environment.
- Understand basic [redacted] that can be used with a Confidential Human Source (CHS)

(S)

b1
b7E

(S)

(S)

b1
b7E

(S)

- Ops Acts

Ops Phone Calls

b1
b7E

(S)

Marking a

(S)

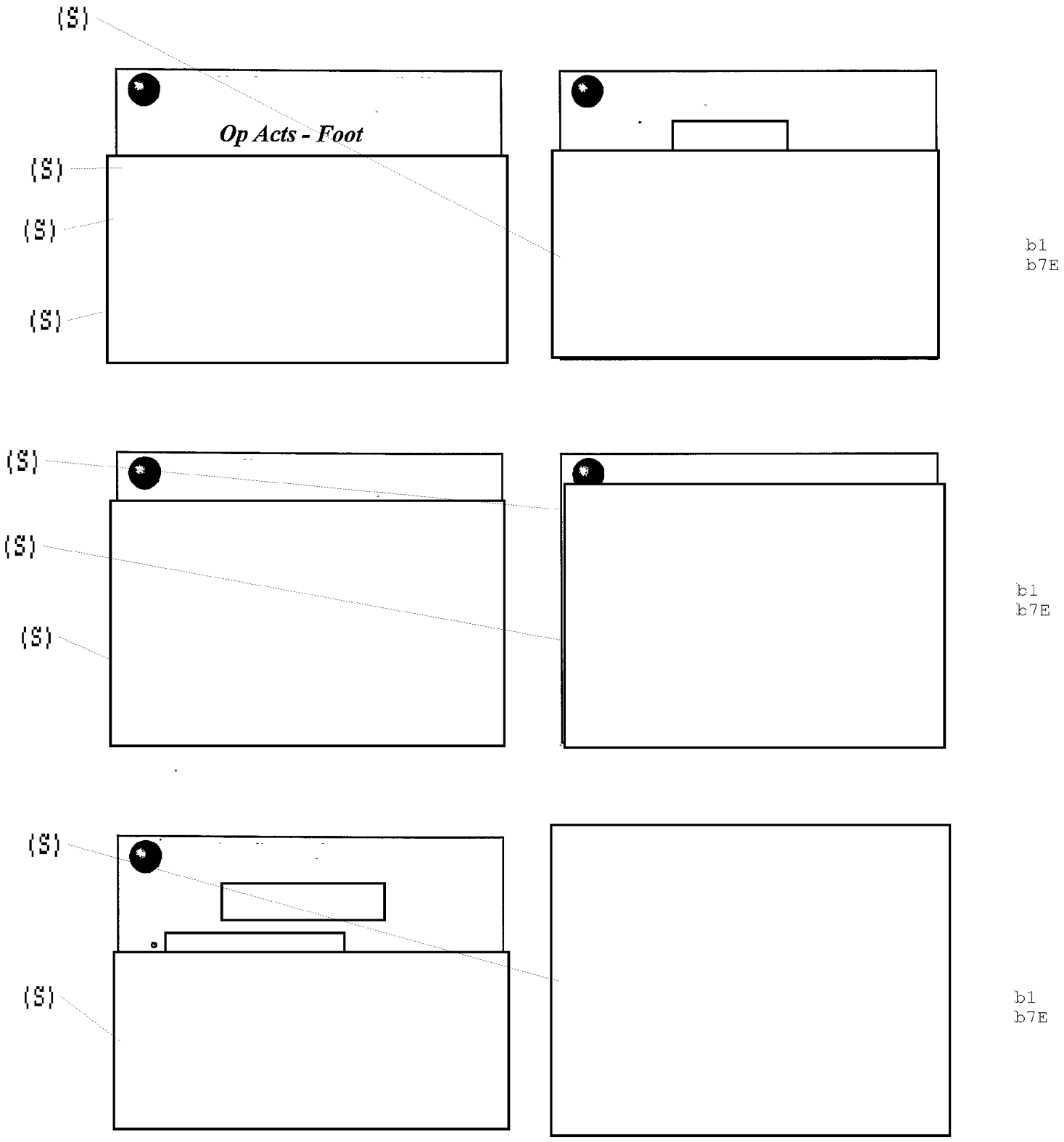
b1
b7E

(S)

(S)

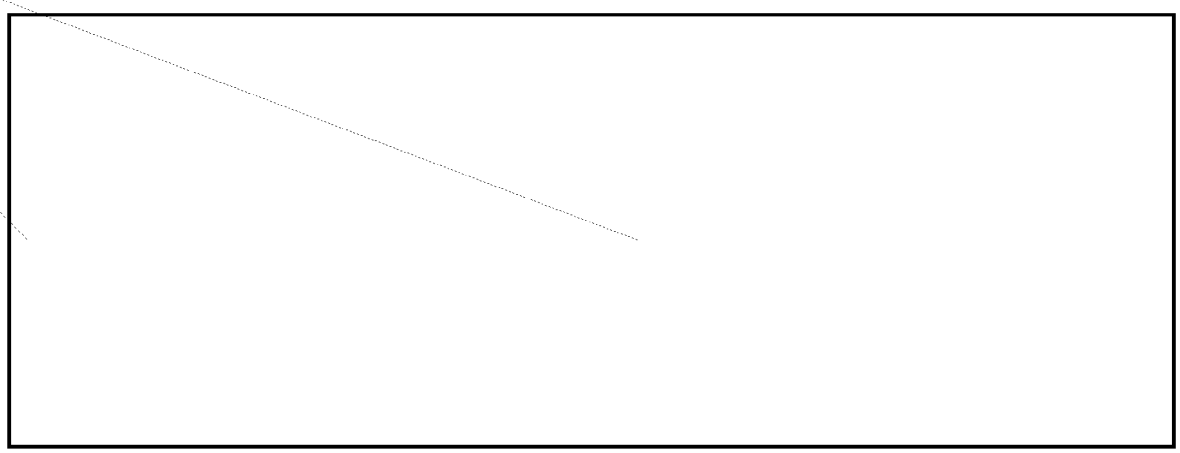
Technical Operations

b1
b7E


(S)
Op Acts - Foot
(S)
(S)
(S)
b1
b7E
(S)
(S)
(S)
b1
b7E
(S)
(S)
b1
b7E

(S)

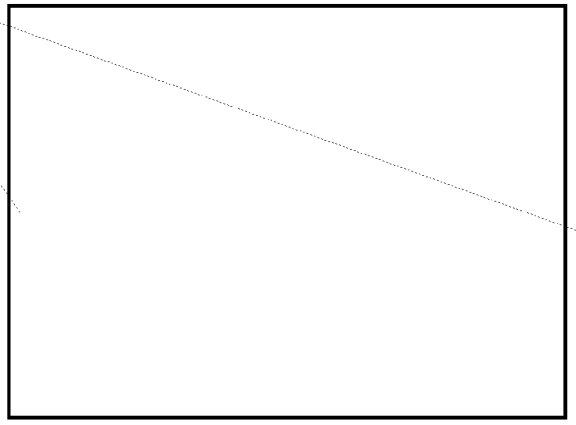
(S)



b1
b7E

(S)

(S)

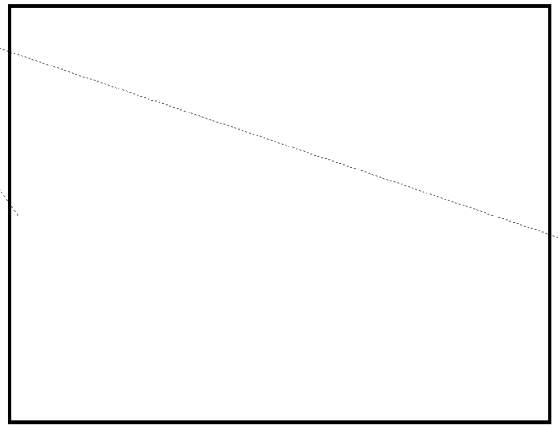


REMEMBER....

b1
b7E

(S)

(S)

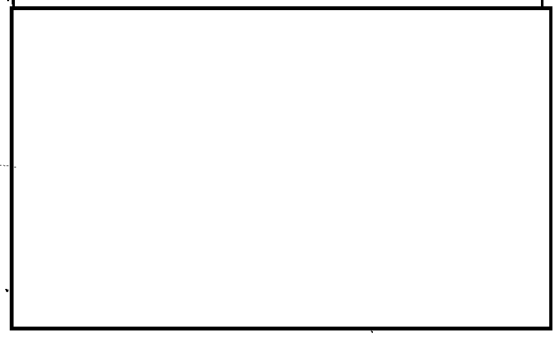


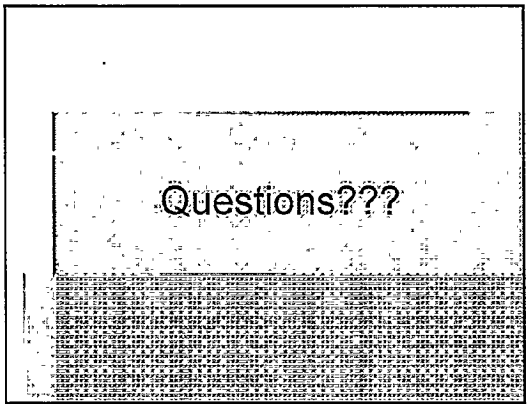
In Short...

b1
b7E

Examples:

(S)

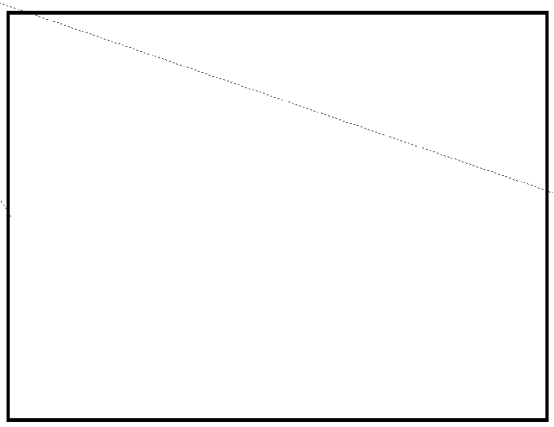


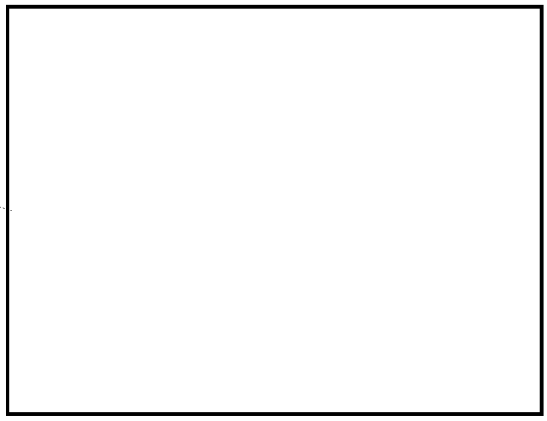


b1
b7E

(S)

(S)

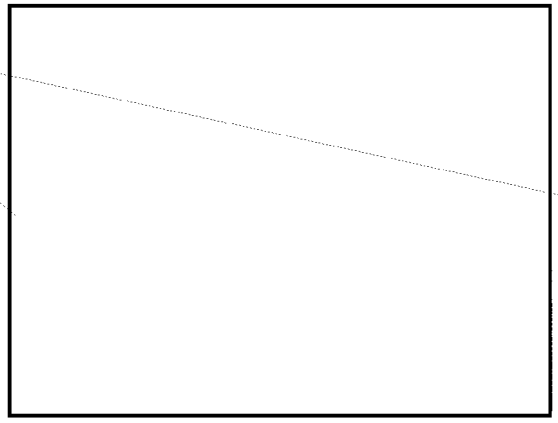


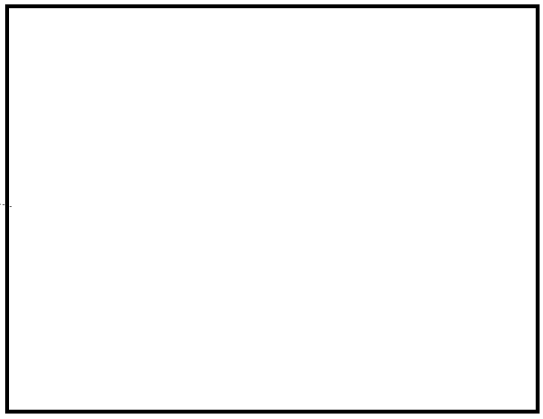


b1
b7E

(S)

(S)

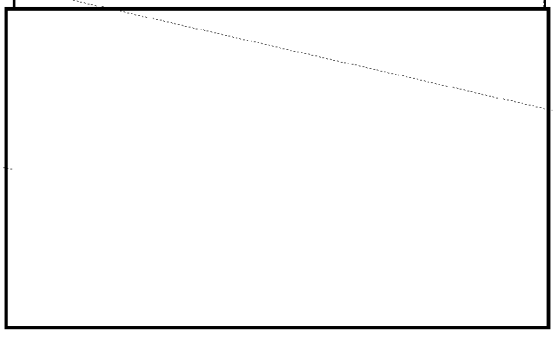




b1
b7E

(S)

Remember



(S)



b1
b7E

(S)

Things to Avoid

(S)

Things to Do

b1
b7E

(S)

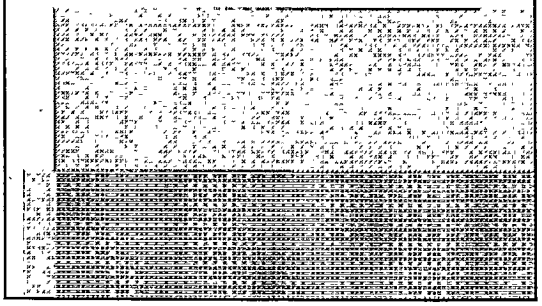
Review

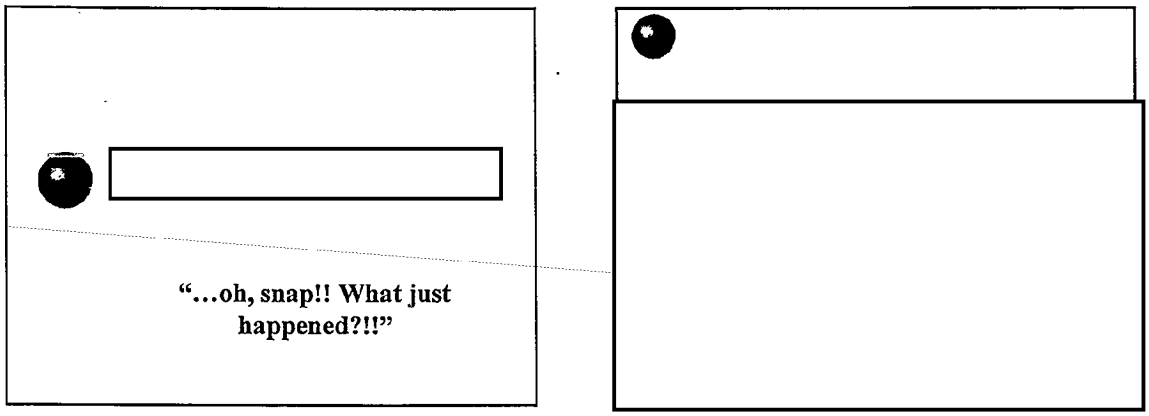
(S)

Review - Overall

b1
b7E

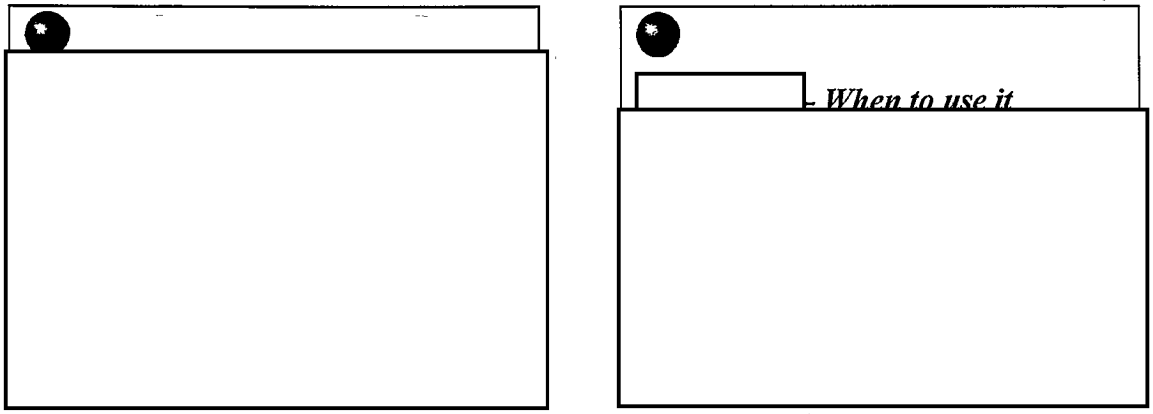
Questions???



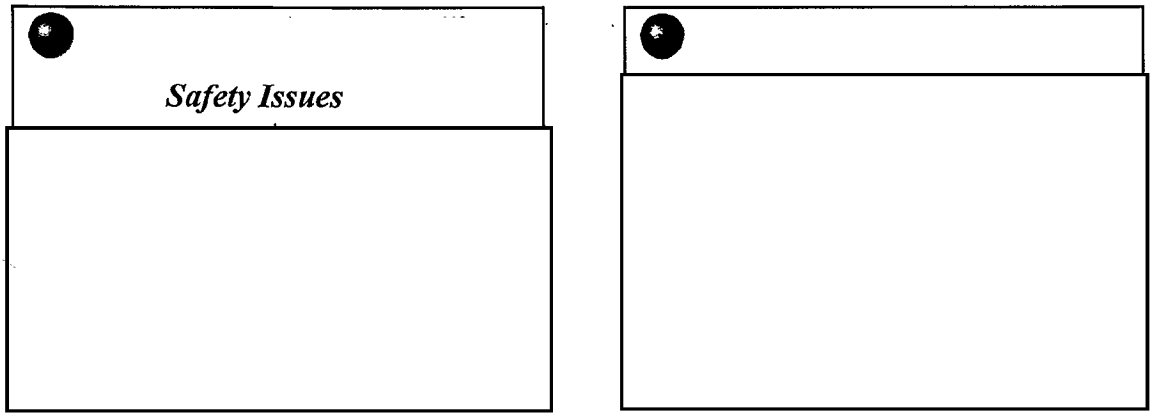


(S)

b1
b7E



b1
b7E

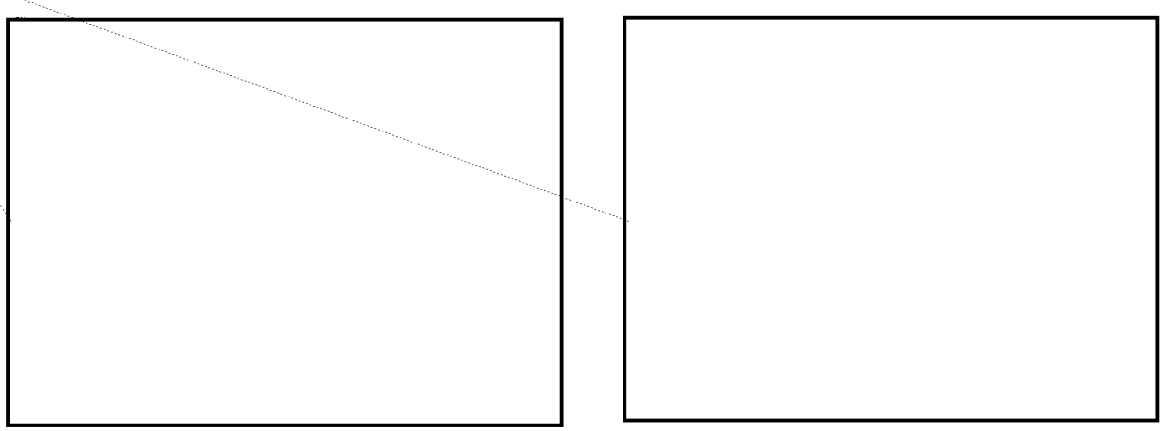


(S)

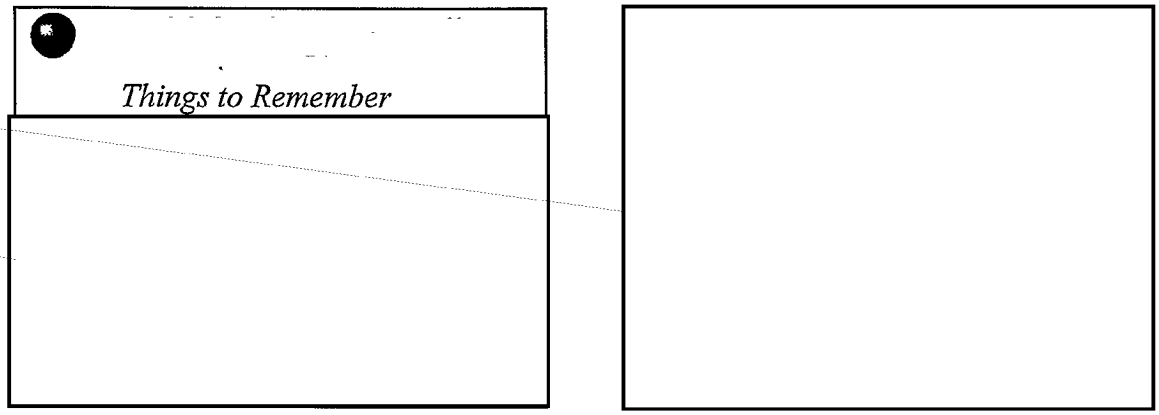
b1
b7E

(S)

(S)



b1
b7E



(S)

(S)

b1
b7E

DATE: 01-09-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Area Familiarization &

For Surveillance

SSA

~~For Official Use Only~~

Area Familiarization

It's just one slice of the TACtical Surveillance Pie.

For Official Use Only

b6
b7C
b7E

For Official Use Only

Lesson Overview

In this lesson you will learn systematic area familiarization an

For Official Use Only

b7E

Objective

At the end of this lesson you will be able to:

(1) Use the *system of area familiarization*

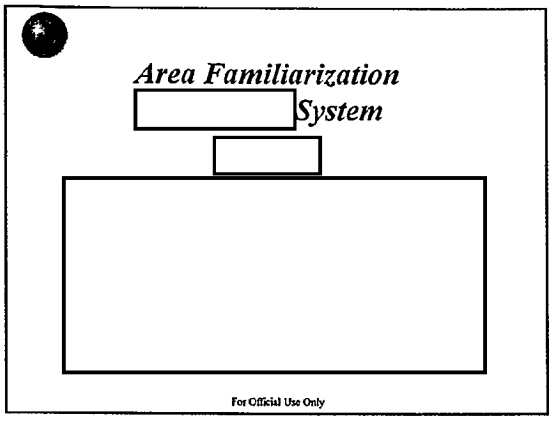
(2)

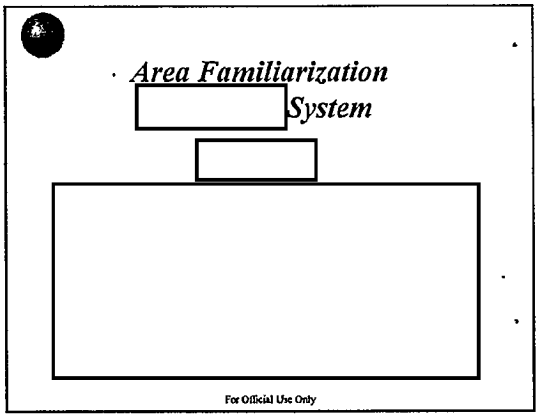
For Official Use Only

Area Familiarization *System Categories*

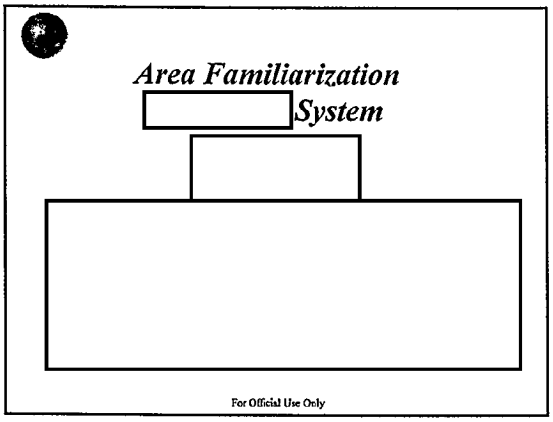
For Official Use Only

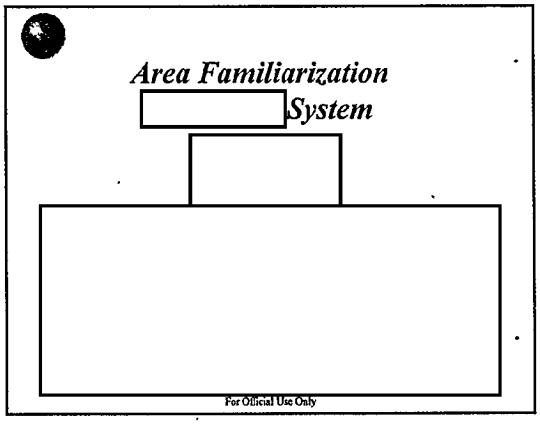
b7E


Area Familiarization
System
For Official Use Only

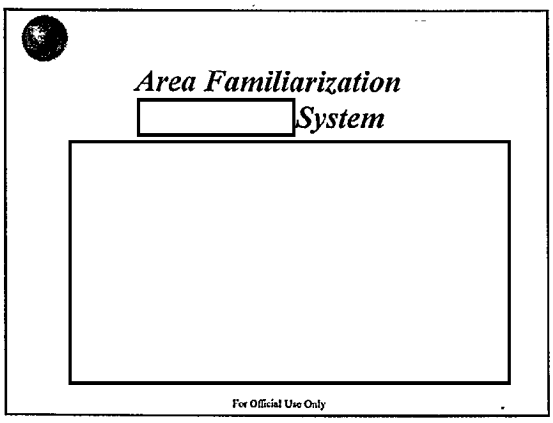

Area Familiarization
System
For Official Use Only

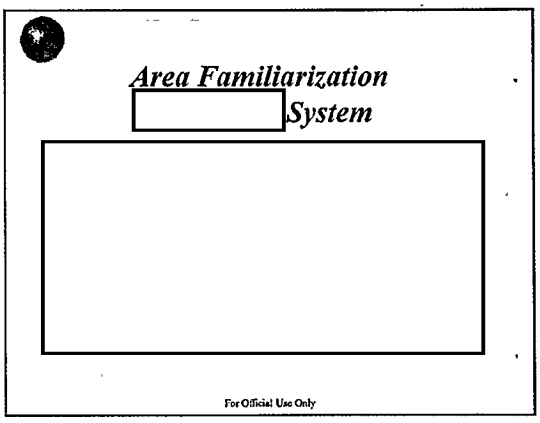
b7E


Area Familiarization
System
For Official Use Only


Area Familiarization
System
For Official Use Only

b7E


Area Familiarization
System
For Official Use Only


Area Familiarization
System
For Official Use Only

b7E

Before you hit the street,
[redacted] *it "on-line"*

[redacted]

For Official Use Only

Correlate [redacted] *research with*
[redacted] *to ensure safety*

[redacted]

-Any others ??

For Official Use Only

b7E

(S) [redacted]

For Official Use Only

[redacted]

b1
b7E

(S) *Now Hit the Street !! (1)*

[redacted]

(S) [redacted]

Now Hit the Street !! (2)

[redacted]

-Start working your [redacted] report
-Notate all parking lots
-Notate the Visitor Centers

~~For Official Use Only~~

b1
b7E

(S)

Now Hit the Street !! (3)

(S)

-Continue working the [redacted] report with more specifics

For Official Use Only

Now Hit the Street !! (4)

[redacted]

-Continue/Complete [redacted] report

For Official Use Only

b1
b7E

Return to office (5)

-Return and study the [redacted] report

- Don't waste it - it's your work

(S)

[redacted]

Getting there is half the fun, right?? "ROAD TRIP!!!!"

[redacted]

For Official Use Only

b1
b7E

Questions??

Good Luck and Have Fun!!

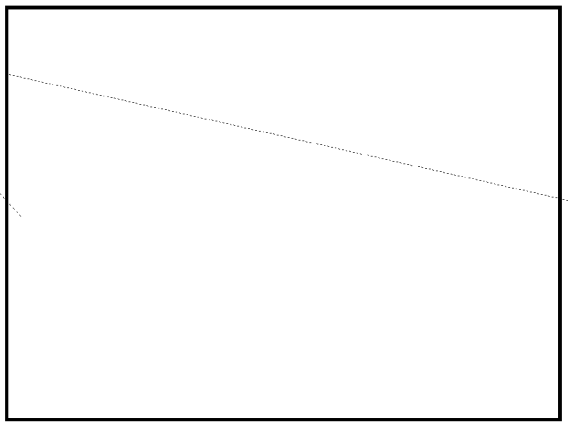
For Official Use Only

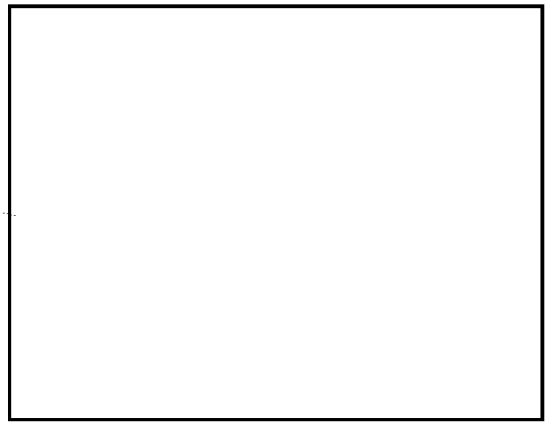
DATE: 01-09-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)



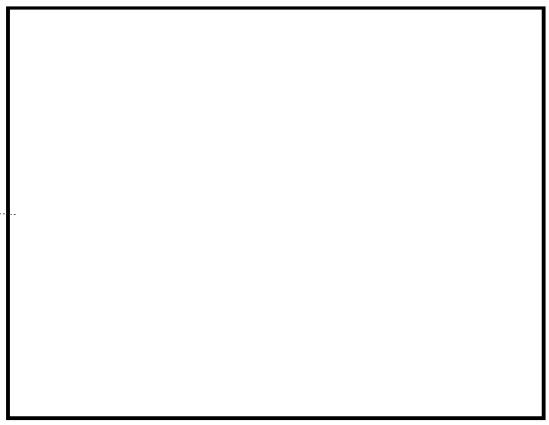


b1
b7E

(S)

Area Familiarization

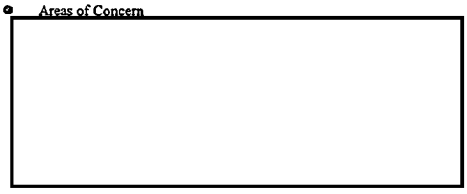
"You know, it's like he had been here before, but we know this is his first trip to the U.S. He must be a quick study."



b1
b7E

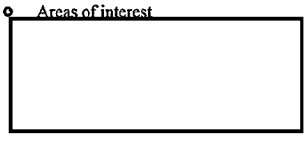
Overt Information

- Maps
  - Local area maps
  - Internet
- Areas of Concern



Overt Information Continued (2)

- Areas of interest



- Mass transportation
  - Buses
  - Subways
  - Trains

b7E

ACLURM032016

FBI031536

(S)

Overt Information Continued (3)

- Other

b1
b7E

(S)

(S)

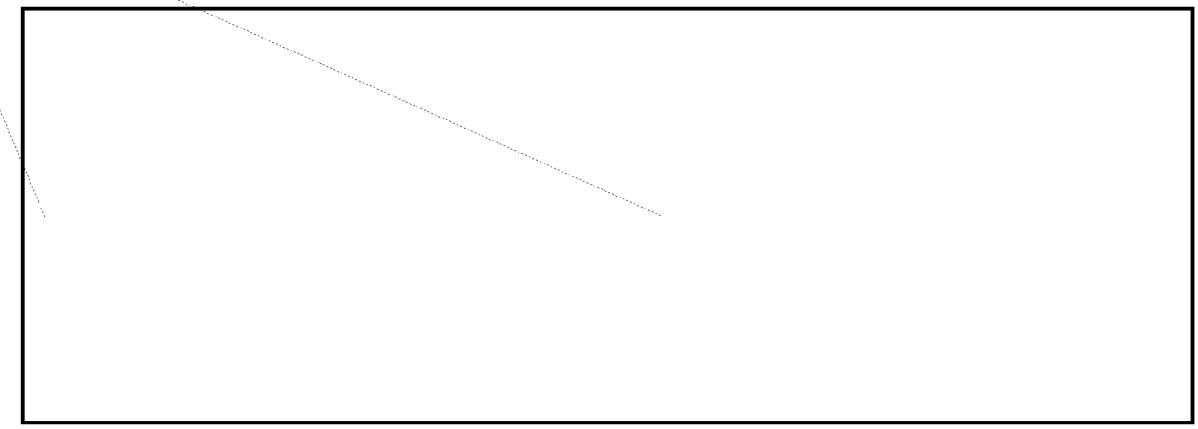
b1
b7E

(S)

(S)

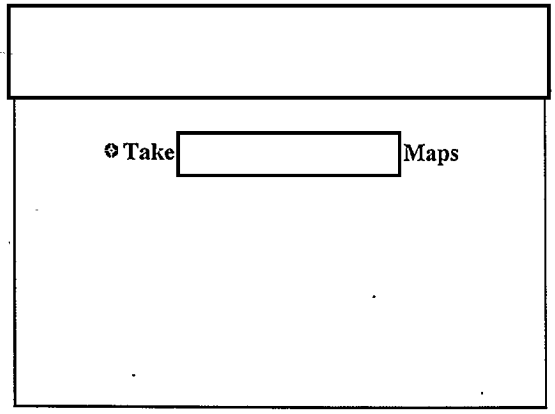
(S)

(S)



b1
b7E

(S)



b1
b7E

ACLURM032018

(S)

26	**Teaching Point:**
(S)	
	Comment:
(S)	b1 b7E
27	**Teaching Point:** To acquaint the student with the concept of **Comment:** (Examples of Ames and Hanssen) b7E
28	**Teaching Point:** To acquaint the student with **Comment:** (Lonetree and Hanin Cases)
29	**Teaching Point:**
(S)	
(S)	**Comment:** Give examples including the Walker and Earl Pitts cases). Jerry Whitworth, John Walker's friend It is doubtful that he thought that but, if he did, would that reduce his criminal liability? b1 b7E
30	**Introduction**
(S)	
31	**Teaching Point:**
(S)	

		Comment
(S)		
	32	**Teaching Point**
(S)		
		Comment
(S)		
	33	**Teaching Point**
(S)		
		Comment
(S)		
	34	**Introduction to Segment re Spy Cameras**
	35	**Comment**
	36	**Segment re Concealed Devices**
	37	**Teaching Point** A variety of common devices found in many homes or offices have been used to secrete intelligence.

b1
b7E

b1
b7E

b7E

	Comment A variety of common, everyday devices have been utilized by intelligence services to enable their agents to conceal information and equipment. Several of these devices appear on this and the following slides.
38	**Teaching Point** The situation drives the design of the concealment.
39	**Comment** Again, a common item used to conceal something used in espionage.
40	**Comment** Everyone has one or more of these.
41	**Introduce Segment re [redacted] is Countered**
42	**Teaching Point** (S) [redacted] b1 b7E **Comment** The methods that will be discussed are listed on the slide.
43	**Teaching Point** (S) [redacted] **Comment** (S) [redacted]
44	**Teaching Point** (S) [redacted] b1 b7E **Comment** (S) [redacted] Mention also: [redacted]

(S)	45	**Teaching Point** **Comment**
(S)	46	**Teaching Point** **Comment** Describe the Verona Case and what it revealed about Soviet intelligence operations and activities in the US. Julius and Ethel Rosenberg were guilty. Point out how difficult it is today to break encrypted messages.
(S)	47	**Teaching Point** **Comment**
(S)	48	**Comment**
(S)	49	**Teaching Point** **Comment**
(S)		

b1
b6
b7C
b7E

b1
b7E

b1
b7E

Teaching Point:

(S) 50

Comment

(S)

b1
b7E

Teaching Point:

(S) 51

Comment

(S)

52 **Teaching Point**

(S)

b1
b7E

Comment

(S)

53 **Training Point**

(S)

Comment

b1
b7E

DISCUSS THE BENEFITS OF RECRUITMENT citing cases involving Oleg Gordievsky, Boris Yuzhin, Kim Philby, and Vasili Mitrokhin.. Discuss the impact of the Robert Hanssen case on the FBI and of the Aldrich Ames case on the CIA.

(S)

(S)

	Photos are of Arkady Shevchecnko, Mitrokin, Philby, Guy Burgess, Donald Maclean, Ed Howard, Ames, Hanssen, Felix Block, Dmitri F. Polyakov, Valeri Martynov, and Sergei Motorin .

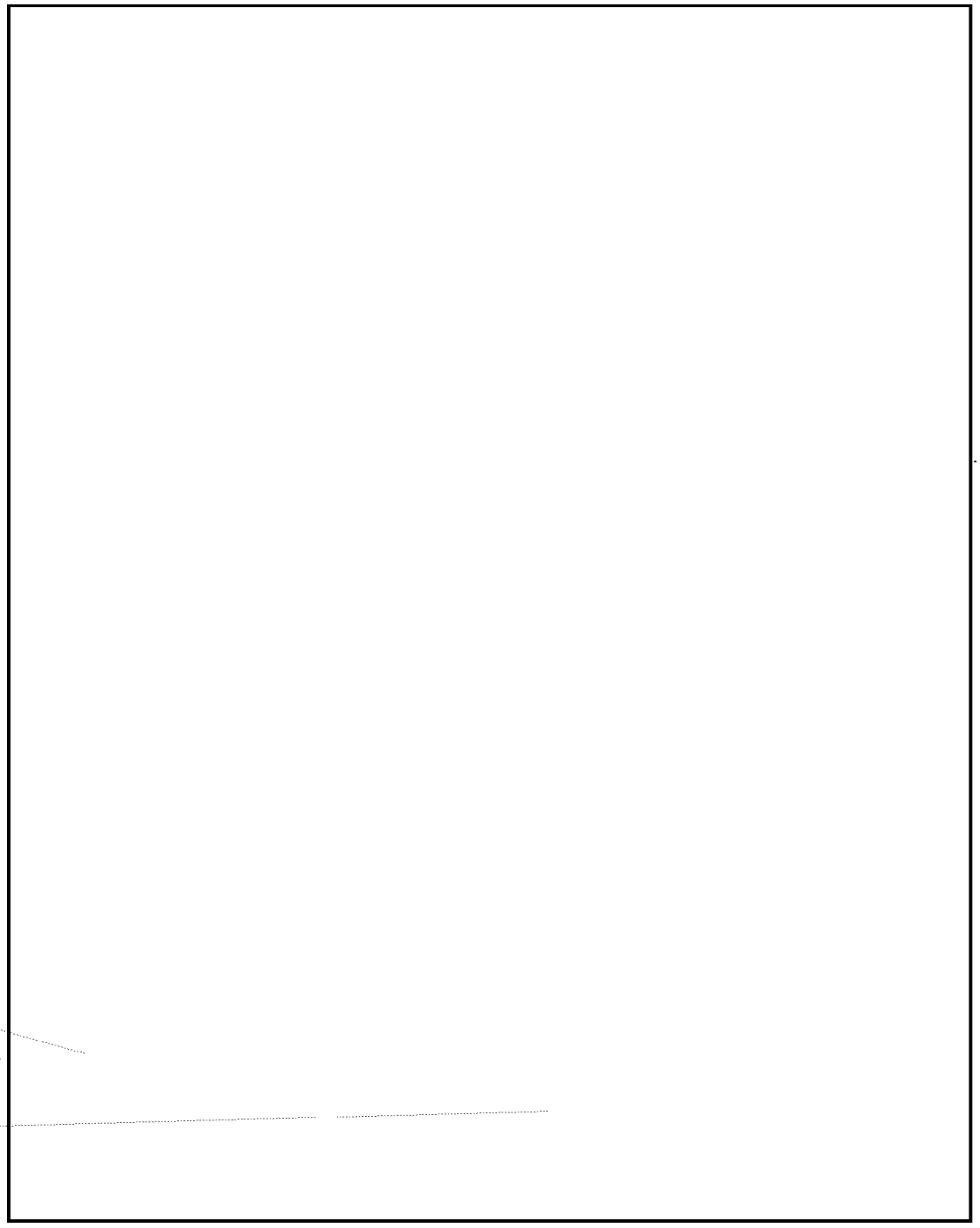
b1
b7E

Criterion Test Questions:

(S)

b1
b7E

Test Answers:



b1
b7E

(S)

(S)

Equipment:

Equipment/Aids for Instructor: Power Point Projector and VHS

Equipment/Aids Required for Instructor: Power Point projector and VCR

Equipment/Aids Required for Students: None.

Power Point Slides or Overheads: Power Point Slides.

Handouts: Yes.

Bibliography:

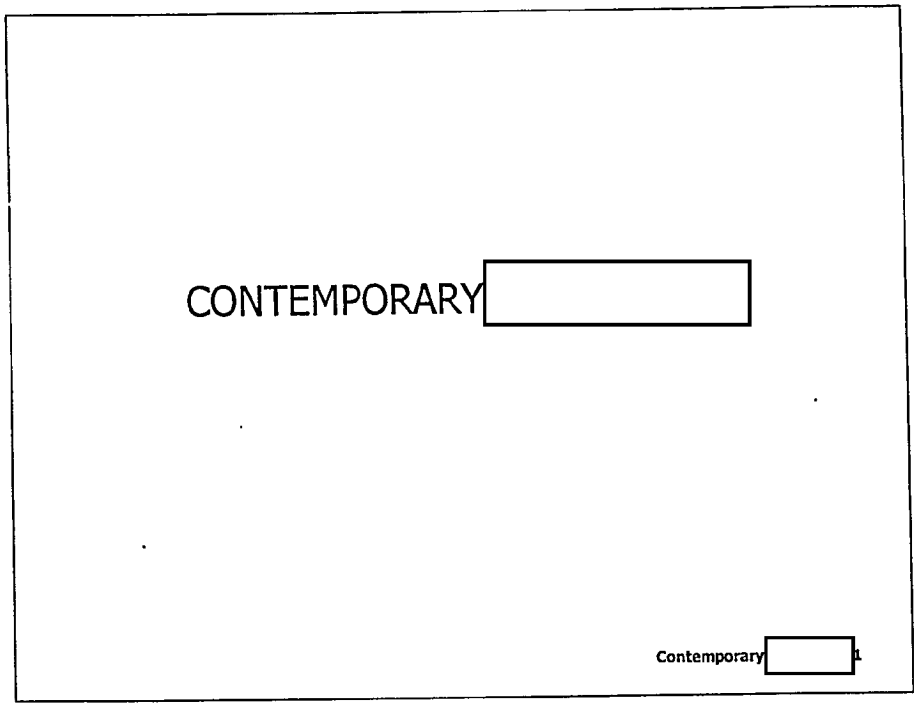
Ronald Kessler. *Moscow Station*. New York: Charles Scribner's Sons, 1989.

Ronald Kessler. *The Spy in the Russian Club*: Charles Scribner's Sons, 1990.

Sherry Sontag and Christopher Drew. *Blind Man's Bluff*. New York: Public Affairs, 1998.

DATE: 01-09-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c,d)
DECLASSIFY ON: 01-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b7E

Agenda

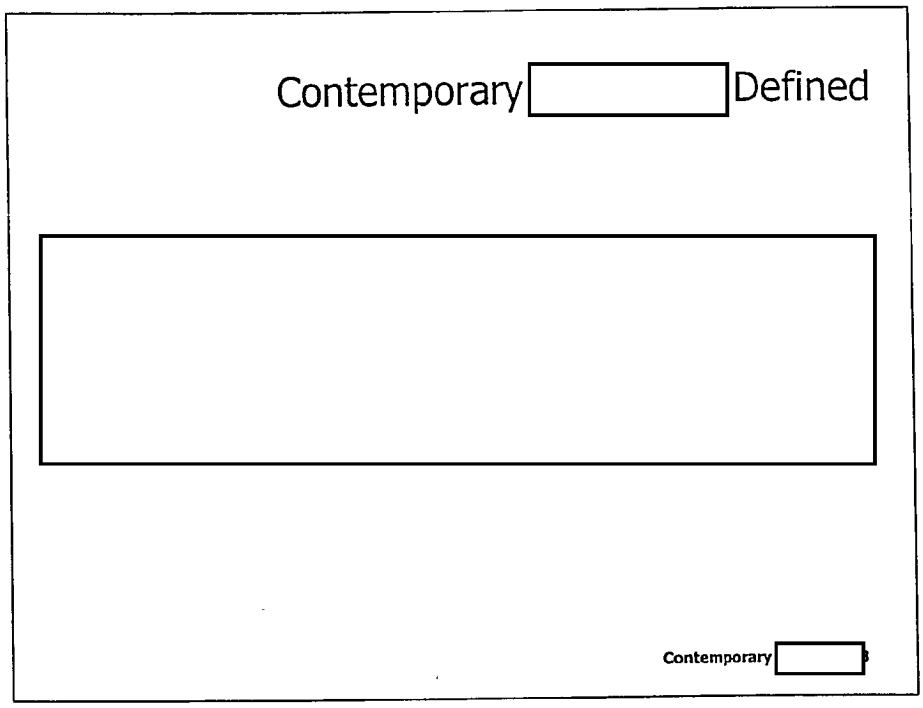
1. Contemporary [redacted] Defined
2. Old Spies and New Focus
3. Old Problems and New Techniques
4. Cyber Attacks
5. Stenanography
6. Satellite Interception
7. Gizmos

Contemporary [redacted] 2

b7E

Comment

Agenda for presentation. See slide.



b7E

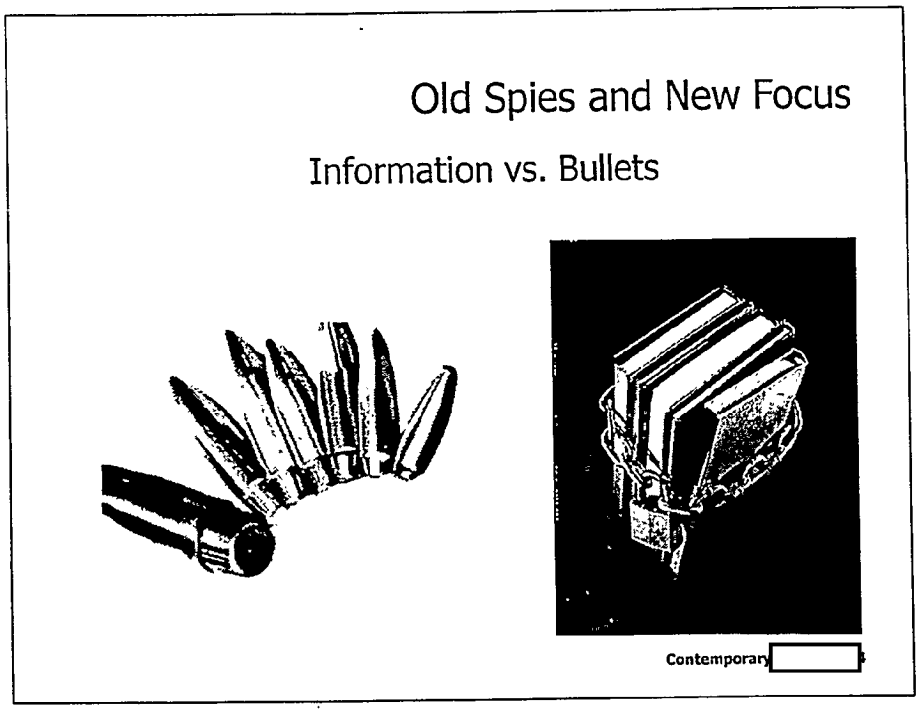
Teaching Point

b7E

Provide student a definition of "contemporary [redacted]"

Comment

See slide.



b7E

Teaching Point

Information pertaining to technology, business and science has replaced military information as the most important focus of intelligence services operating throughout the world.

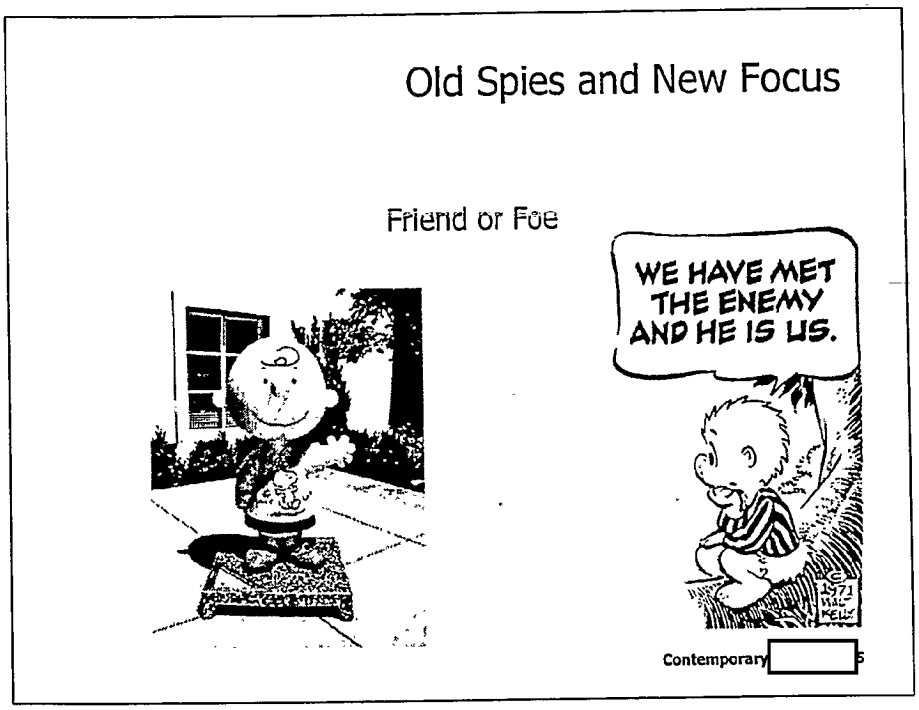
Comment

In the final days of the Cold War, the crumbling Soviet Union possessed the nuclear weapons to destroy the world but lacked the economic and informational infrastructure to compete as a world power. While the preeminent weapon for most of this century was the hydrogen bomb, it has been replaced by the awesome capability of a single electron! Future superpowers will be those nations with the greatest capability to harness the power of the electron for both economic and "digital" warfare.

The desire of foreign spies to uncover and obtain "military secrets" will continue, but with variations. We are witnessing the migration of a national defensive infrastructure that has historically been based on "bullets" into one based upon "information." Success by spies targeting an opponent's "information" will ultimately prove more valuable.

New technologies are changing the traditional methods and techniques, the [redacted] by which spies operate. b7E

1 http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/



b7E

Teaching Point

With the end of the Cold War, the strong East vs. West alignment in the world has diminished leading to a redefinition of intelligence based on national interests.

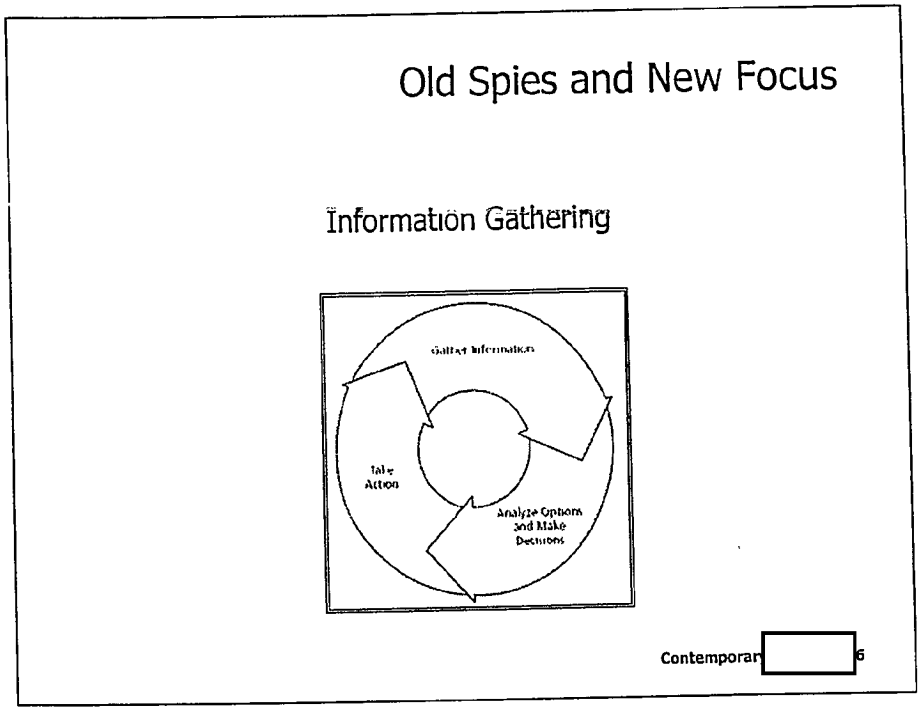
Comment

Even at the height of Cold War solidarity (the enemy of my enemy is my friend), the major superpowers collected intelligence and attacked the ciphers, or codes, of our friends as well as our enemies. The national interests of former friends and foes are now being redefined in terms of competing economic interests.

Some observers believe that cultural and historic friendships between nations will continue to fade as they are replaced by trading partnerships and other interdependent economic relationships. The friend of my enemy may also be my friend -- if the price is right. Military alliances will be designed to protect, perpetuate and enhance underlying economic partnerships. The victors in global economic warfare will form regional economic alliances that will share information and together strengthen their collective -- and individual -- economic power.

Gen. Yuri Kobaladze of the SVR -- the Russian Foreign Intelligence Service, successor to the First Chief Directorate of the KGB -- recently stated "there are friendly nations, but there are no friendly intelligence services". [1]

1 http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/



b7E

Teaching Point

The traditional methods of collecting and communicating intelligence have changed in ways that could not be imagined just a few years ago.

Comment

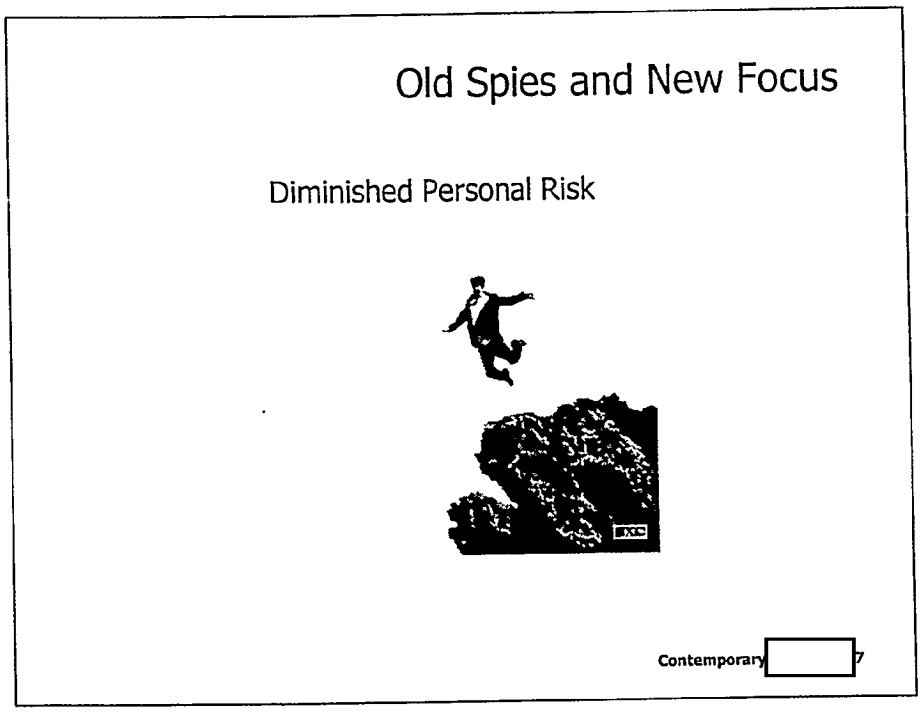
The following outlines some technology advances that have dramatically impacted intelligence services' methods:

1. Satellite collection. The satellite program began nearly 30 years ago provided the United States with the capability to digitally observe events on Earth in near "real time."

b7E

2. Communications interception

3. Speech recognition software, new to the consumer market but utilized by intelligence agencies for more than 25 years



b7D
b7E

Teaching Point

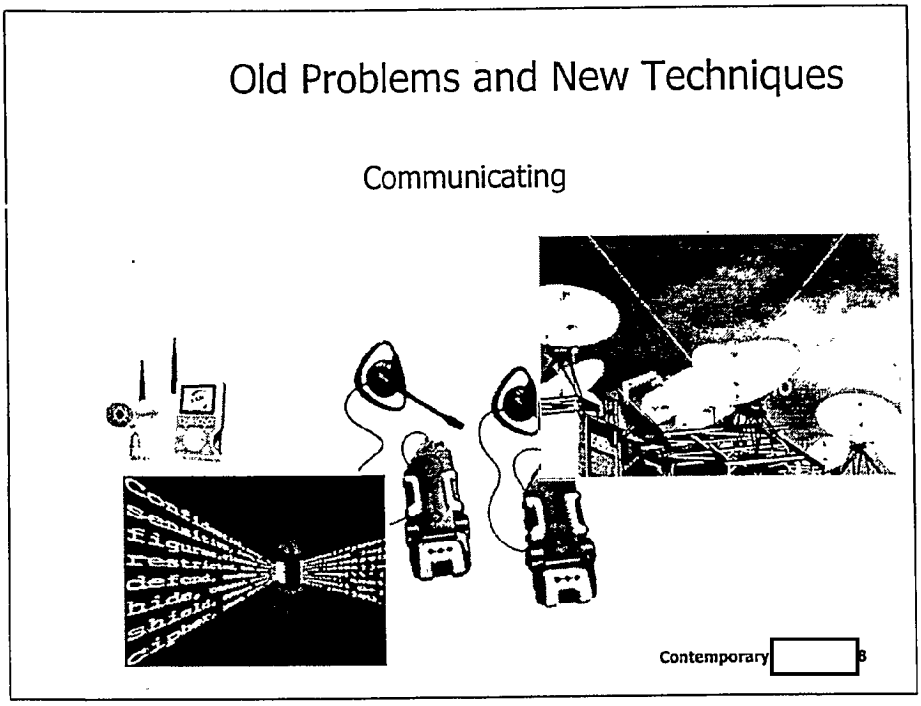
In some important ways, espionage agents can accomplish certain tasks using modern technology that previously required great personal risk.

Comment

During World War II, the OSS (U.S. Office of Strategic Services) and [redacted] coordinated resistance activities in occupied Europe to disrupt [redacted] transportation and manufacturing. These daring individuals risked death to sabotage [redacted]

In the digital world, however, potential targets have shifted. Even with the emphasis of advanced computer developments, all nations depend on imbedded computer chips of varying age -- sometimes decades old. These critically important components control the switching systems in power grids, telephone systems and transportation networks. The devastating effect of losing an antiquated but functioning system becomes a reality when the key person charged with its upkeep is eliminated. The result of assassinating a political leader pales when compared with the effect in future wars of eliminating key computer programmers and network specialists.

For professional intelligence services, their primary goal is, and will remain, the acquisition of information, not murder. Oleg Tsarev, a retired officer of the KGB's First Chief Directorate and author, accurately stated that "intelligence stops when you pick up a gun."



Teaching Point

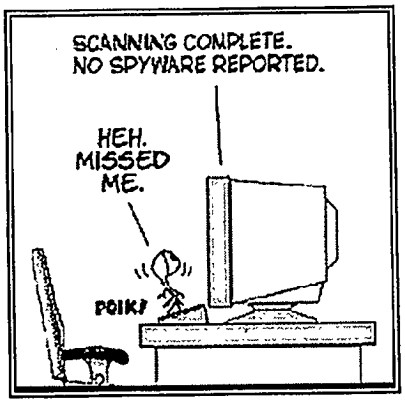
Profound changes in technology have dramatically affected the methods employed to communicate to and from espionage agents.

Comment

Communication of instructions, money and tasking to a spy and of information from the spy to the intelligence service that operates him is, of course, one of the greatest vulnerabilities inherent in an espionage operation. Modern technology [redacted] b7E
[redacted] have presented huge improvements in the ability of spies to communicate and challenges to counterintelligence.

Old Problems and New Techniques

Malware Utilization



Contemporary [redacted]

b7E

Teaching Point

To acquaint the student with use of malware by hostile intelligence services.

Comment

Disruption of the enemy's capabilities has long been a goal of intelligence services.

Wikipedia defines "malware" as software designed to infiltrate or damage a computer system, without the owner's informed consent. The term is a portmanteau of "mal-" (or perhaps "malicious") and "software", and describes the intent of the creator, rather than any particular features. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and some adware. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of California, West Virginia, and several other U.S. states.[1]

In the new world of the digital spy, these same activities can be accomplished, at no personal risk, from a computer terminal thousands of miles away. By digitally sabotaging enemy computer networks, cyber-spies can accomplish the same result as their OSS and [redacted] predecessors. [redacted] vulnerability of the national information infrastructure of most countries -- the interlocking computer [redacted] -- make Pearl Harbor in 1941 appear well protected. At the same time, billions of dollars are being spent to shore up unprotected computer networks, and accelerated programs are being developed to exploit the computer networks of our enemies as we prepare for future "cyber wars."

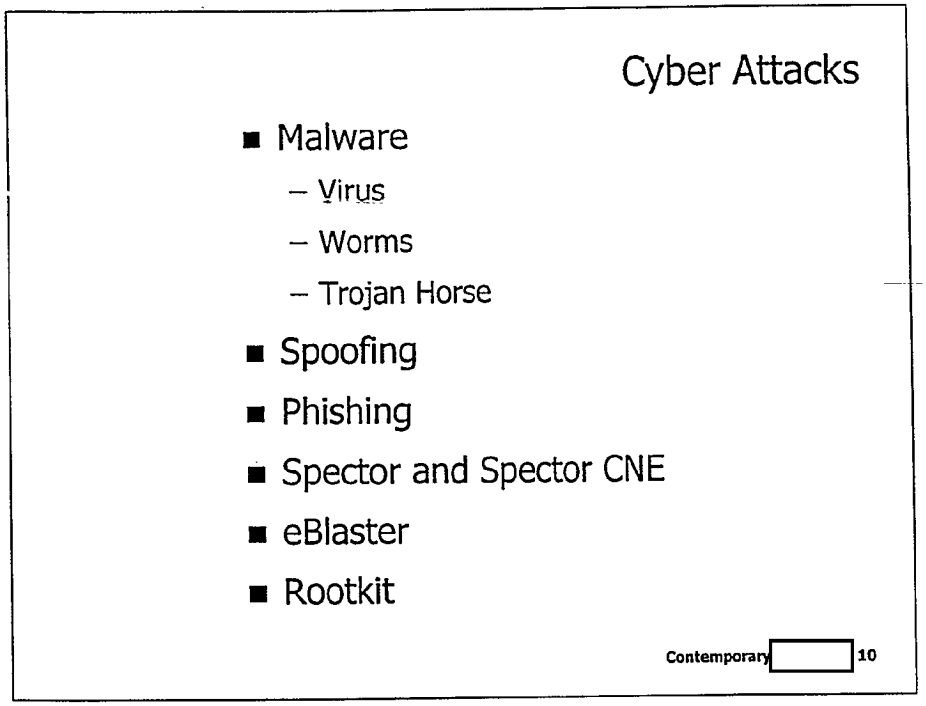
b7D
b7E

[redacted]

[redacted] is over before it has begun.

1 http://en.wikipedia.org/wiki/Malware

ACLURM032035



b7E

Comment

Slide provides outline of what will be covered. Note that only a general description of the technique will be provided as the lecturer is not an engineer.

Cyber Attacks



Virus

A virus is a self-replicating/self-reproducing-automation program that spreads by inserting copies of itself into other executable code or documents.

A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

Extending the analogy, the insertion of a virus into the program is termed as an "infection".

Contemporary [redacted] 11

b7E

Teaching Point

Acquaint students with a computer virus and its potential impact.

Comment

See slide and next two slides.

Cyber Attacks

Virus



The infected file (or executable code that is not part of a file) is called a "host". Viruses generally do not affect network performance, as their malicious activities are mostly confined within the target computer itself.

Viruses are one of the several types of malicious software or malware

Predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

Contemporary [redacted] 12

b7E

Cyber Attacks



Virus

Some viruses have a delayed payload, which is sometimes called a bomb.

For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts.

A time bomb occurs during a particular date or time.

A logic bomb occurs when the user of a computer takes an action that triggers the bomb.

Contemporary [redacted] 13

b7E

Cyber Attacks

Worms



A **computer worm** is a self-replicating computer program, similar to a computer virus.

A worm is self-contained and does not need to be part of another program to propagate itself.

Contemporary [redacted] 14

b7E

Teaching Point

Acquaint students with a computer worm and its potential impact.

Comment

See this slide and next slide.

Pictured is Sven Jaschan who was arrested near Rotenberg, Germany, on May 8. He subsequently confessed to creating the Sasser worm. The 18-year-old was apprehended following a tip to Microsoft Corp. from a group of people in the culprit's home state of Lower Saxony.

The Wikipedia defines the **Sasser worm** as a computer worm that affects computers running vulnerable versions of the Microsoft operating systems Windows XP and Windows 2000. Like other recent worms, Sasser spreads by exploiting the system through a vulnerable network port.

The effects of Sasser include the news agency Agence France-Presse (AFP) having all its satellite communications blocked for hours and the U.S. flight company Delta Air Lines having to cancel several trans-atlantic flights because its computer systems had been swamped by the worm.[1]

1 http://en.wikipedia.org/wiki/Sasser_worm

Cyber Attacks

Worms

They are often designed to exploit the file transmission capabilities found on many computers.

The main difference between a computer virus and a worm is that a virus cannot propagate by itself whereas worms can.

A worm uses a network to send copies of itself to other systems and it does so without any intervention.

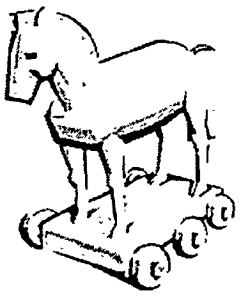
In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer.

Contemporary [redacted] 15

b7E

Trojan Horse

Cyber Attacks



- **A Trojan horse** is a malicious program that is disguised as legitimate software.
- The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

Contemporary [redacted] 16

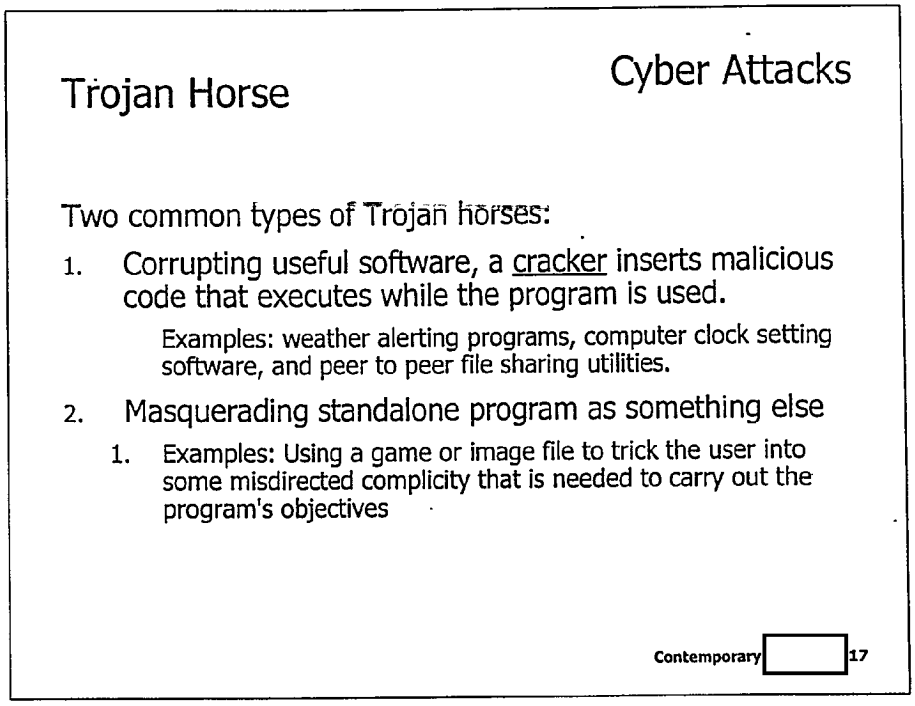
b7E

Teaching Point

To acquaint the student with the concept of the Trojan horse program.

Comment

Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. Just as the Greeks needed the Trojans to bring the horse inside for their plan to work, Trojan horse programs depend on actions by the intended victims. As such, if trojans replicate and even distribute themselves, each new victim must run the program/trojan. Therefore their virulence is of a different nature, depending on successful implementation of social engineering concepts rather than flaws in a computer system's security design or configuration



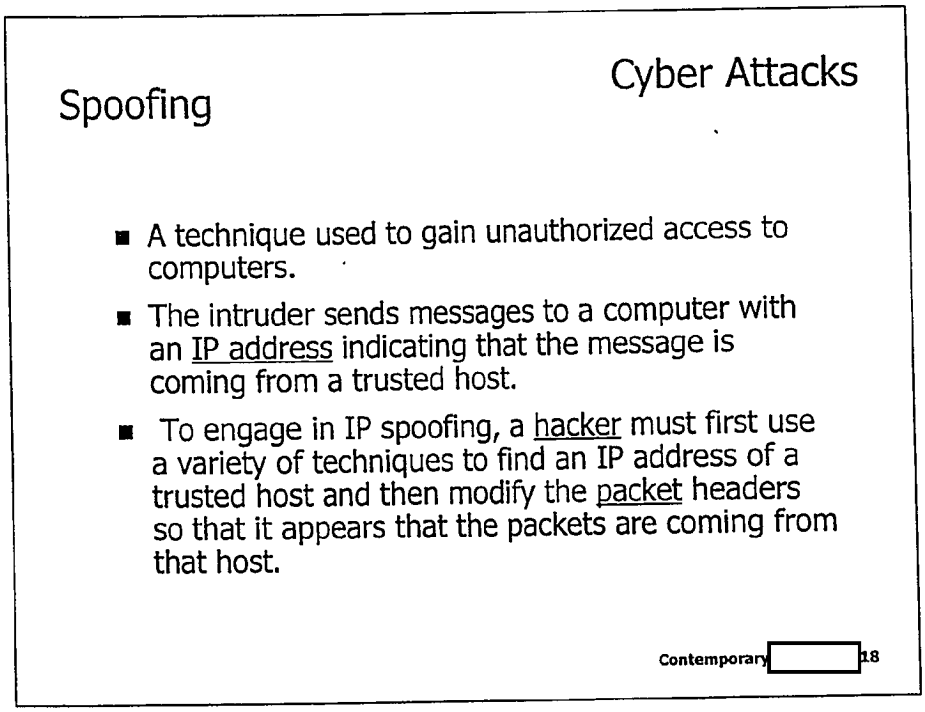
b7E

Teaching Point

To acquaint the student with the concept of the Trojan horse program.

Comment

See slide.



b7E

Teaching Point

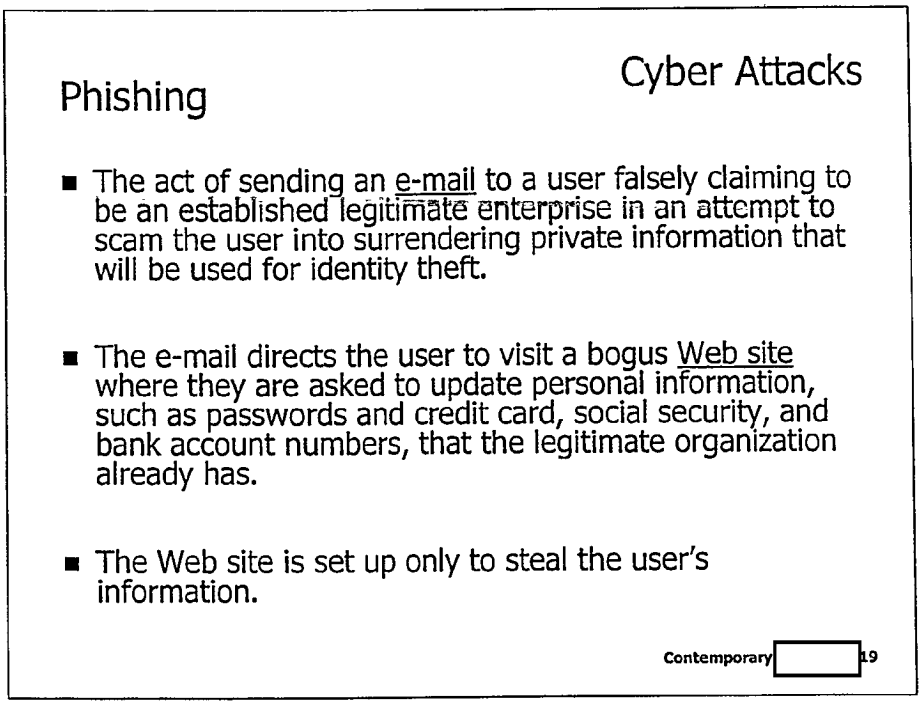
To acquaint the student with the technique of computer spoofing and its potential use by an intelligence service.

Comment

From the FBI website: "IP Spoofing" is a technique used to gain unauthorized access to computers, whereby the intruder sends a message to a computer with an IP address indicating that the message is coming from a trusted port.

Spoofing is generally used as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. Spoofing also often involves trademark and other intellectual property violations.

b7E



b7E

Teaching Point

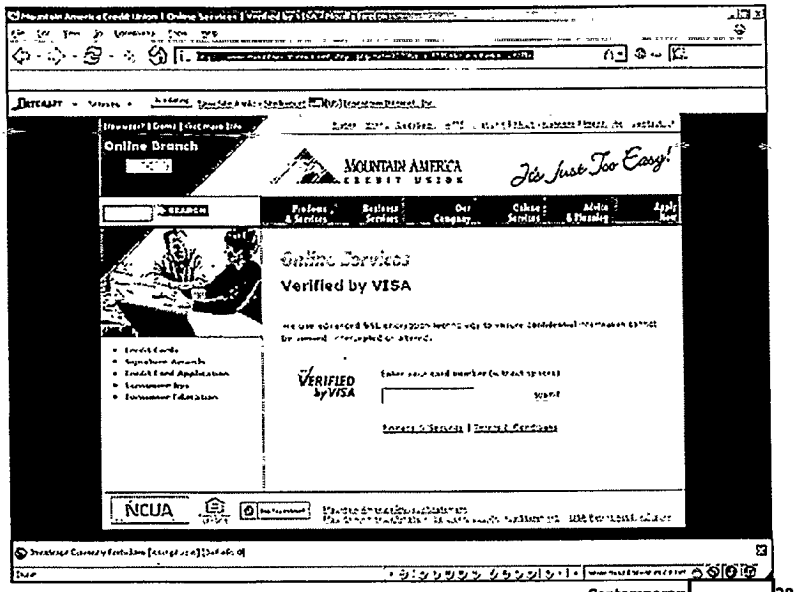
To acquaint the student with the technique of computer phishing and its potential use by an intelligence service.

Comment

According to Computer World, phishing isn't really new -- it's a type of scam that has been around for years and in fact predates computers. Malicious crackers did it over the phone for years and called it social engineering. What is new is its contemporary delivery vehicle -- spam and faked Web pages.

Phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with -- banks such as Citibank; online organizations such as eBay and PayPal; Internet service providers such as AOL, MSN, Yahoo and EarthLink; online retailers such as Best Buy; and insurance agencies. The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. [1]

[1] See http://www.computerworld.com/securitytopics/security/story/0,10801,89096,00.html



Contemporary 20

b7E

Teaching Point

To acquaint the student with the technique of computer phishing and its potential use by an intelligence service.

Comment

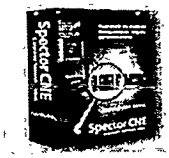
The following from the *Washington* Post, (By Brian Krebs | February 13, 2006; 1:50 PM ET). A source recently forwarded a link to one of the "best" phishing attacks I've ever seen. This one -- targeting the tiny **Mountain America** credit union in Salt Lake City, Utah -- arrives in an HTML-based e-mail telling recipients that their Mountain America credit union card was automatically enrolled in the Verified by Visa program, a legitimate security program offered by Visa that is supposed to provide "reassurance that only you can use your Visa card online."

The e-mail includes the first five digits of the "enrolled card," but those five digits are found on all Mountain America bank cards, so that portion of the scam is likely to be highly convincing for some recipients. The message directs readers to click on a link and activate their new Verified by Visa membership.

Now here's where it gets really interesting. The phishing site, which is still up at the time of this writing, is protected by a Secure Sockets Layer (SSL) encryption certificate issued by a division of the credit reporting bureau **Equifax** that is now part of a company called **Geotrust**. SSL is a technology designed to ensure that sensitive information transmitted online cannot be read by a third-party who may have access to the data stream while it is being transmitted. All legitimate banking sites use them, but it's pretty rare to see them on fraudulent sites.

Cyber Attacks

Spector CNE - Corporate Network Edition



Spector and Spector CNE

- The Most Intelligent Internet Monitoring and Surveillance Software available. Rated #1 spy software by PC Magazine.
- Records Emails, Chats, IMs, Web Sites, Programs Run, Keystrokes Typed, Peer to Peer File Sharing, Screen Snapshots –

  Plus - Offers Internet Access Blocking and Instant Notification Alerts.

Contemporary [redacted] 21

b7E

Teaching Point

To acquaint the student with the technique of monitoring the use of computers.

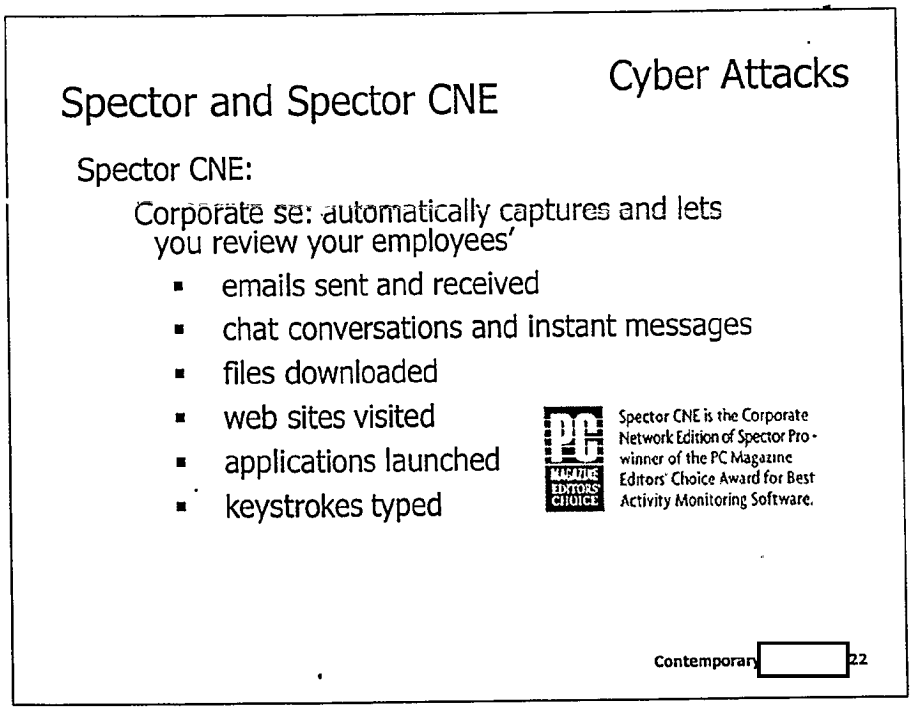
Comment

Immediate email alerts notify you whenever certain words (and phrases) you specify are typed by the user or are contained in an email, chat, instant message or a web site. (Spector CNE's email recording is so comprehensive that it covers Outlook, Exchange, AOL, Hotmail, Yahoo and any SMTP/POP3-based architecture.)

Spector CNE can be remotely configured and installed FROM any computer on the network TO any computer on the network, and the recordings can be viewed from any PC on the network.

[redacted]

b7E



b7E

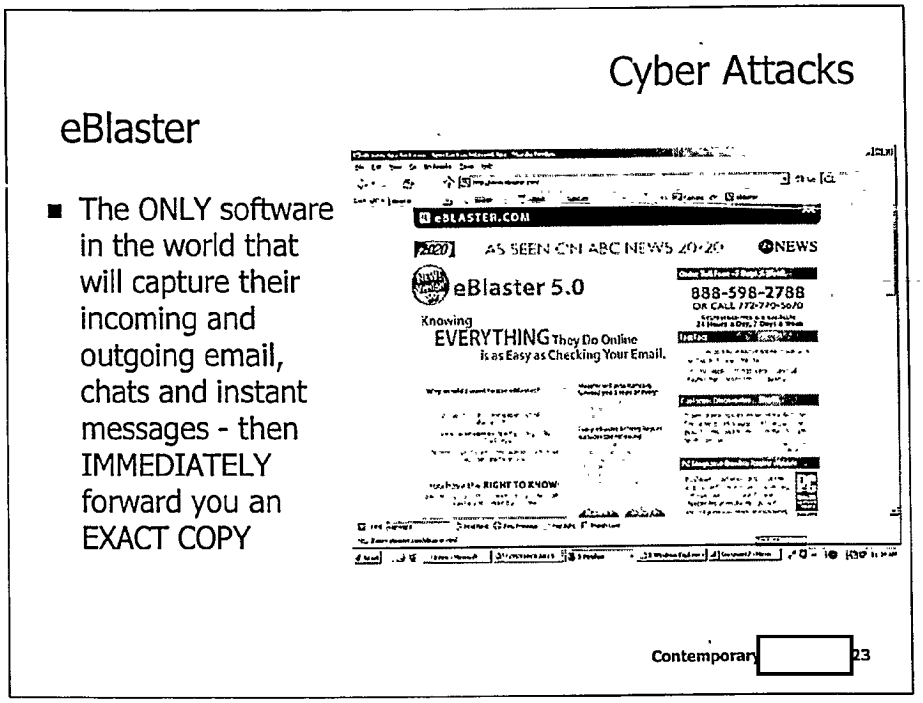
Teaching Point

To acquaint the student with the technique of monitoring the use of computers.

Comment

See slide for comments.

In addition, by taking screen snapshots, Spector CNE creates the equivalent of a digital surveillance tape so that you can see the exact sequence of everything your employees are doing on the computer.



b7E

Teaching Point

To acquaint the student with various commercial techniques of monitoring the use of computers.

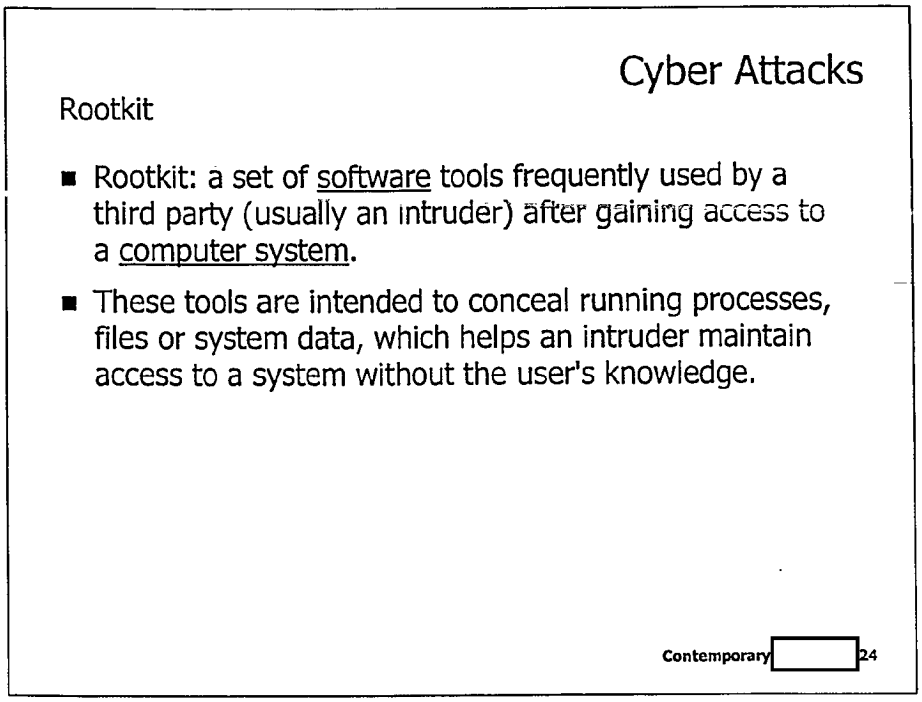
Comment

Slide depicts eBlaster website and the claim that it can monitor "everything they do on line as easy as checking your email." the site also provides the following "example:"

- *You are at work and your child is home from school.*
- *She receives an email from John at 3:00 PM.*
- *Within seconds, you receive a COPY of that email sent to your email address.*
- *A few minutes later, she replies to John's email.*
- *Within seconds, you receive a COPY of what she sent to John.*

In addition, eBlaster spy software records ALL emails, chats, instant messages, web sites visited, keystrokes typed, programs launched and peer-to-peer (P2P) files downloaded - then sends it to you via email in the form of a detailed Activity Report.

Receive your Activity Reports as frequently as once every hour or once a day - it's your choice.



b7E

Teaching Point

To acquaint the student with the rootkit which can be used to conceal running processes, files or system data, thereby helping an intruder to maintain access to a system whilst avoiding detection. the use of computers.

Comment

Definition of: rootkit on this slide and next slide.

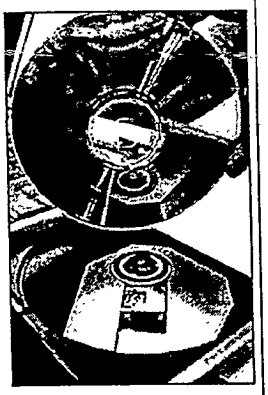
Discuss in relation to the Regan and Hanssen cases.
A type of Trojan that keeps itself, other files, registry keys and network connections hidden from detection. It enables an attacker to have "root" access to the computer, which means it runs at the lowest level of the machine. A rootkit typically intercepts common API calls. For example, it can intercept requests to a file manager such as Explorer and cause it to keep certain files hidden from display, even reporting false file counts and sizes to the user. Rootkits came from the Unix world and started out as a set of altered utilities such as the ls command, which is used to list file names in the directory (folder).

The word "rootkit" came to public awareness in the 2005 Sony CD copy protection scandal, in which Sony BMG music CDs surreptitiously placed a rootkit on Microsoft Windows PCs when the CD was played on the computer. Sony provided no mention of this in the CD or its packaging, referring only to security rights management measures.

Cyber Attacks

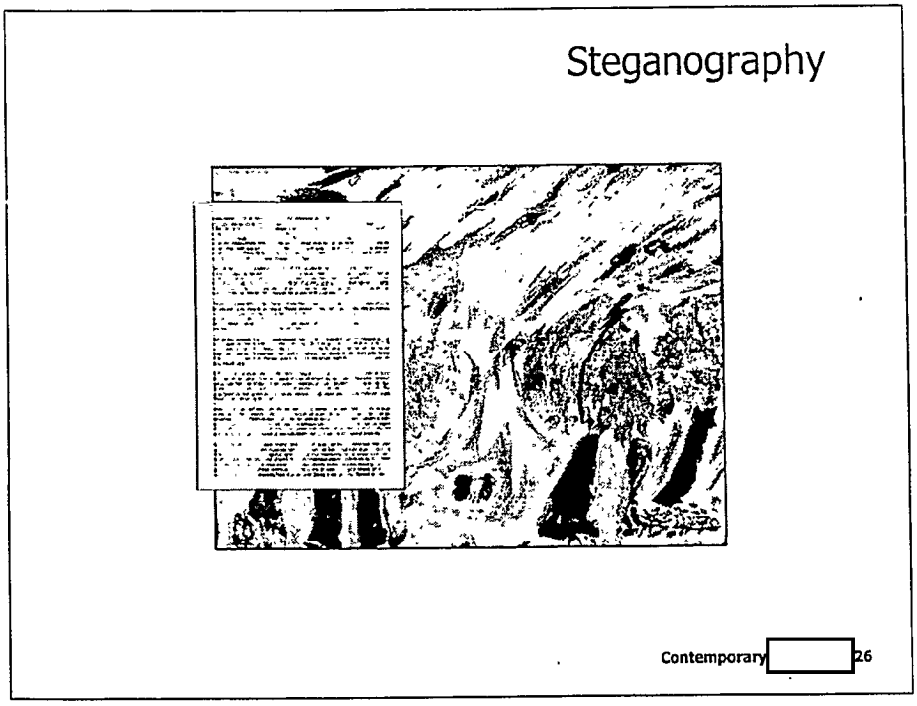
Rootkit

- Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows.
- A computer with a rootkit on it is called a rooted computer.
- The word "rootkit" came to public awareness in the 2005 Sony CD copy protection controversy, in which Sony BMG music CDs placed a rootkit on Microsoft Windows PCs



Contemporary [redacted] 25

b7E



b7E

Teaching Point

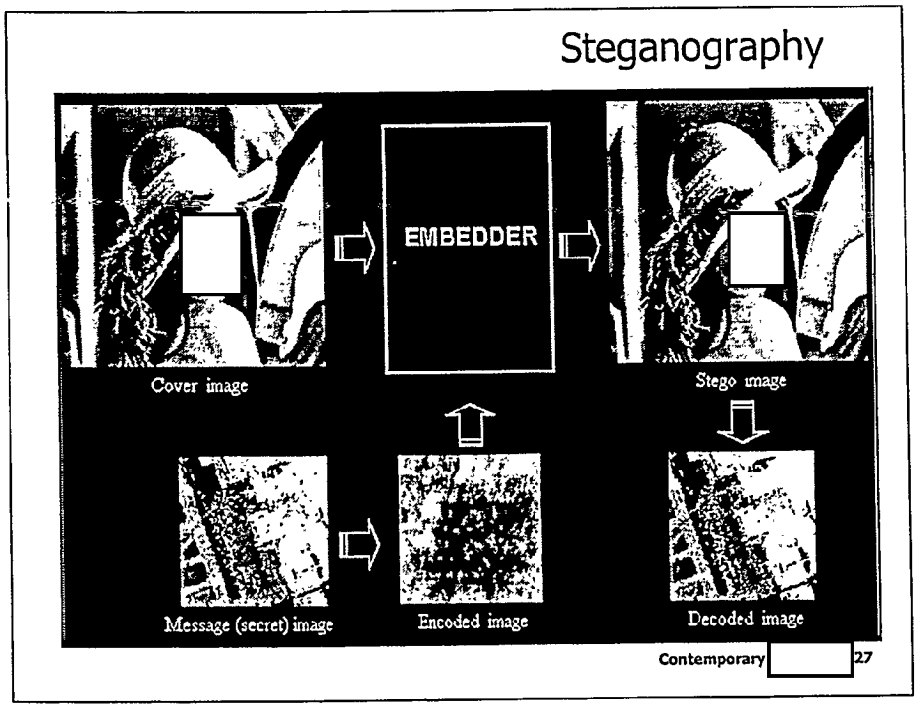
To acquaint the student with steganography which can be used to conceal information.

Comment

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured.[1]

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend. A recording of a short sentence might contain your company's plans for a secret new product. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking.

[1] http://en.wikipedia.org/wiki/Steganography



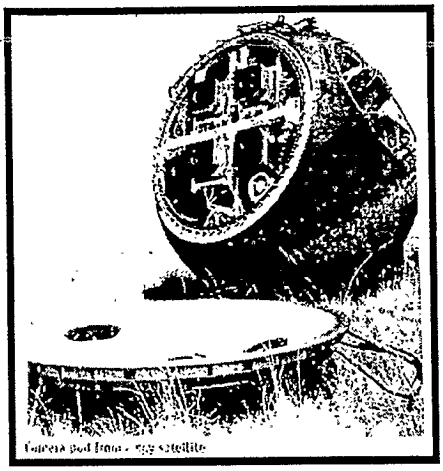
b6
b7C

b7E

Comment

While steganography often borrows ideas from—or works in concert with—encryption, it is not encryption. The aim of encryption is to scramble a message so that a third party cannot unscramble it, even if that third party knows full well that the intercepted communication is encrypted. **The goal of steganography is to hide the fact that a message is being sent in the first place.** Thus, old and new technologies ranging from invisible ink to spread-spectrum communications are forms of steganography. In the digital age, steganography involves techniques that allow the hiding of messages within digital media.

Satellite Audio Interception and Photography



Contemporary [redacted] 28

b7E

Teaching Point

To acquaint the student with use of Satellites for Audio Interception and Photography.

Comment

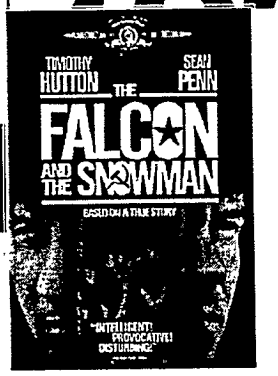
A **spy satellite** (officially referred to as a **reconnaissance satellite** or **recon sat**) is an Earth observation satellite or communications satellite deployed for military or intelligence applications. Until the 1970s and even the 1980s, many reconnaissance satellites that took photographs would eject canisters of photographic film, which would descend to earth and be retrieved in mid-air as they floated down on parachutes.[1]

The first satellites ejected canisters.

1 http://en.wikipedia.org/wiki/Reconnaissance_satellite

Satellite Audio Interception and Photography





Contemporary [redacted] 29

b7E

Training Point

Provide the student an understanding of the basic facts of the espionage case pertaining to Andrew Daulton Lee and Christopher Boyce who compromised US satellite systems.

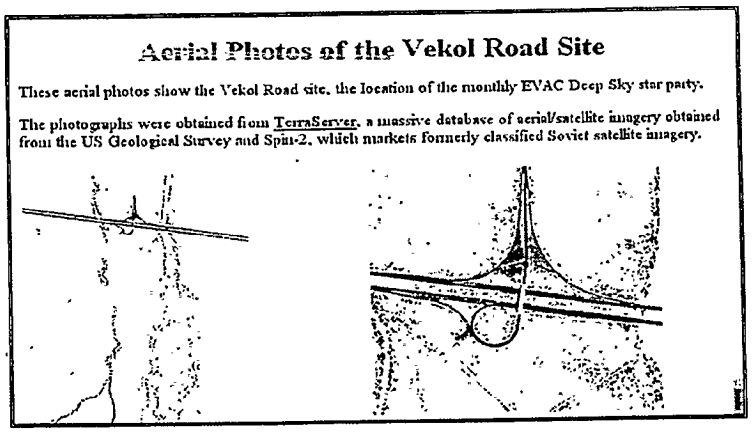
Comment

Andrew Daulton Lee and Christopher Boyce. United States citizens and Los Angeles natives, were portrayed by actor Sean Penn in director John Schlesinger's 1985 movie *The Falcon and the Snowman* based on the book by Robert Lindsey. The book and the film documented the true to life espionage activities of Lee (a heroin and cocaine dealer by trade, hence his nickname, "The Snowman") and his childhood friend Christopher Boyce during the mid-1970s. The Boyce character (nicknamed "The Falcon" because of his long interest in the sport of falconry) was played in the film by actor Timothy Hutton.

For nearly two years, Lee (the adopted eldest son of a wealthy physician) traveled to Mexico City operating as the courier for an espionage scheme which had consisted of his delivering to Soviet Embassy officials classified documents concerning how to decrypt secure US government message traffic and detailed specifications of the latest US spy satellites. These documents were supplied by Boyce, a code clerk employed with the large US defense contractor TRW, headquartered in the Los Angeles community of Redondo Beach. Boyce (whose father was an aerospace corporation security officer and a retired FBI agent) held a top secret clearance and worked in the company's "Black Vault" (classified communications center.)[1]

[1] http://en.wikipedia.org/wiki/Andrew_Daulton_Lee

Satellite Audio Interception and Photography



Contemporary [redacted]30

b7E

Teaching Point

To provide an understanding of the wide use of satellite photography to collect intelligence.

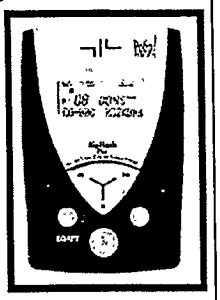
Comment

East Valley Astronomy Club – Star club uses the TerraServer to place instructions on line for its parties. The photos on the Terraserver were taken by Soviet spy satellites.

Audio Gizmos

RipFlashtm Plus Features:

MP3/WMA (Windows tm Media Audio) Player and MP3 Recorder 128MB Four Hour CD Quality (WMA) Playback (2hourMP3 Record) Up to 30 Hour Voice Recording (MP3 encoded)



Backlit Display with full ID3 tag data

Compact size ; 2.32 x 3.46 x0.67 in (WxHxD)

Built -in Microphone and Speaker (MP3 Voice Recording)

Line-in for direct recording from any analog audio source

Smart Media Card Memory Expansion Slot

Contemporary [redacted]31

b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of effective devices that can be used to collect and communicate intelligence information.

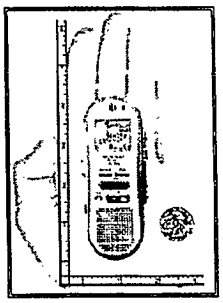
Comment

See slide for description of device.[1]

[1] www.asisonline.org/lac/executive/teletech.ppt

Audio Gizmos

Olympus DS-660 Features:



32MB of built-in memory; up to 11 hours recording time.

USB docking station

Voice Activation -- automatically begins and stops recording as it senses volume

Recording time: SP mode - 5 H; LP mode – 11 H

Site – 108 x 41.5 x 21 mm

Weight – 75g (including batteries)

Contemporary [redacted] 32

b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

New Audio Recorders with USB connectivity.

See slide for description of device.[1]

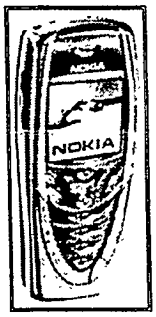
[1] www.asisonline.org/lac/executive/teletech.ppt

ACLURM032058

FBI031578

Audio Gizmos

Spy Phone (Unlocked) » $1,799.00
Standard
Triband GSM: 1900 / 900 / 1800 (Works Worldwide)
Weight 76g, **Dimensions**102mm x 44mm x 13mm
Display Monochrome,
Battery Talk Time: 300 mins, Standby: 260 hrs
Features



- Built in Speakerphone
- You can listen in on whoever takes the spy phone at anytime.
- Can dial out and receive any phone call, like any other cell phone.
- Transmission occurs only when the eavesdropper calls the cellular bug from a preprogrammed number.

Contemporary [redacted]33

b7E

Teaching Points

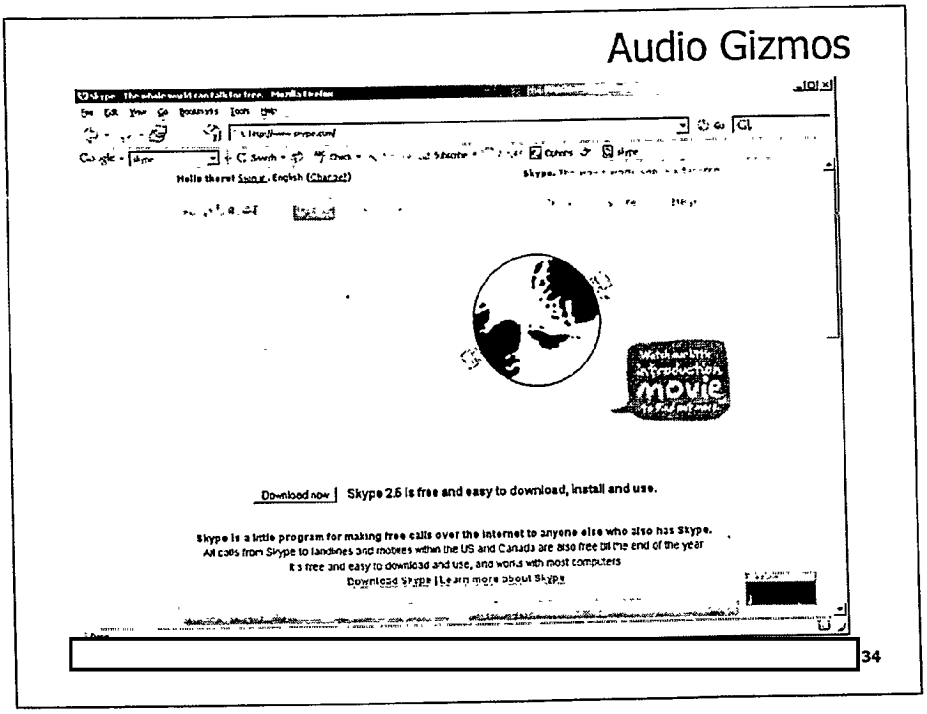
To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

The telephone is programmed with a telephone number and when anyone calls the spy phone, it rings and operates as a normal telephone but when the phone is called using the telephone with the number that was previously programmed into the spy phone, it automatically answers without any ringing or lights coming on and the display stays the same as if it is on ordinary standby. There is no other spy telephone available that can do all this. This phone can be used with any sim card.

By a simple press of a button, a seemingly standard cell phone device switches into a mode in which it seems to be turned off. However, in this deceitful mode the phone will automatically answer incoming calls, without any visual or audio indications whatsoever. In most cases, such spy phones are concealed within the targeted area, for instance, inside a houseplant. A well placed bug phone can be activated on demand from any remote location (even out of another country). Such phones can also prove valuable in business negotiations. The spy phone owner leaves the meeting room, (claiming a restroom break, for instance), calls the spy phone and listens to the ongoing conversation. On return the owners negotiating positions may change dramatically.

Available in a dual band model for Europe as well.



b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

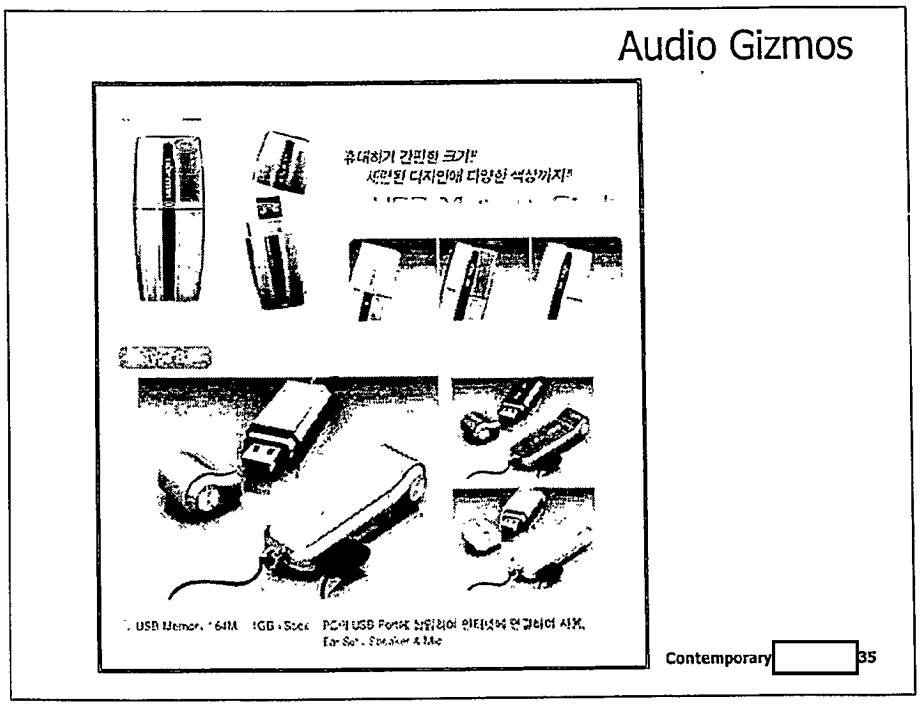
Comment

VoIP is nothing new, in fact services such as Skype have made it easy, cheap as well as extremely popular. In order to beat such service, it is obvious that new entrants are going to need several tricks up their sleeve to woo the customers.

The following is from the skype.com FACs:

Is Skype secure?

> *Yes. When you call another Skype user your call is encrypted with strong encryption algorithms ensuring you privacy. In some cases your Skype communication may be routed via other users in the peer-to-peer network. Skype encryption protects you from potential eavesdropping from malicious users.*



b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Ubistar (An Korean company) has some up with just what the doctor ordered. They are selling memory sticks (most of us have these) in capacities that range from 64 megabytes right up to 1 Gb. These memory sticks can carry the software for connecting to the internet and using a VoIP system. Since most of us need and carry these anyway, there is no additional hardware that you are being asked to tag along.

The only thing that adds to the stick is the microphone and ear phones. Ubistar offers the device in a choice of 3 colors - Green, Pink & Silver. The phone dialer comes along with the memory stick and needs to be loaded on the PC. Simply plug in the memory stick into the USB port and attach the ear phones. As with other VoIP systems you can be connected to another PC, landline or cell phone. Vice-versa, these people can also contact you on your IP phone. An added benefit that Ubistar has thrown is that of allowing you to send MMS, SMS and e-mails with the software that comes along with. Its an excellent idea, one which justifies buying the VoIP memory stick all by itself.

Audio Gizmos

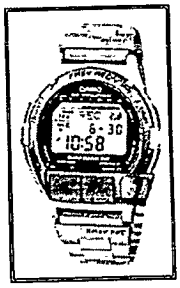
Casio Audio Recorder:

30 Second Record capability

30 Pages of TeleMemo Data

$69

MP3 watches also available



Contemporar[redacted]36

b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

See slide.

Video/Photo Gizmos



Micro Camera

- 300 Foot Transmission Range
- Operates on a Single 9 Volt Battery
- Matching Wireless Receiver Included
- Field Of View 60 Degrees
- Pinhole Style Lens
- $79 - $99 with audio capability

Contemporary [redacted] 37

b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

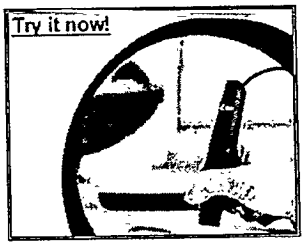
Comment

See slide.

Video/Photo Gizmos

Scanner Pen

- Handheld Scanner
- Top model can store
- 3000 pages of text
- Has IR transfer capability
- $100 - $200



Contemporary [redacted] 38

b7E

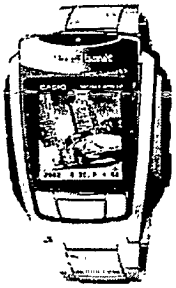
Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

See slide.

Video/Photo Gizmos



Casio Watch Camera:

- ■Recording system JPEG (176 x 144 pixels), 16,770,000- color data
- ■Recording medium Built-in Flash Memory (1 MB)
- ■Memory capacity Up to 100 images*1 (JPEG format); auto memory of shooting date/time
- Focusing distance approx. 30 cm, compensation possible Zoom 2X digital zoom
- Shooting mode Outdoor, Indoor, Dusk; brightness control
- Databank function Up to 24 characters/image (uppercase alphabetic characters, numbers, symbols), thumbnail search function
- IR Data Communication, range 10 cm max Contemporary [redacted] 39

b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

See slide.

Video/Photo Gizmos

Pen Cam Mega P-3

Multi-function : Digital still camera/PC camera/digital camcorder

1.3 megapixel CMOSInternal memory

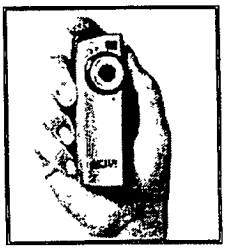
Image capacity - 8 MB built-in SDRAM (for avi movies)116 MB built-in Flash memory (for digital stills)

1248 x 960- up to 50 pictures

640 x 480- up to 160 pictures AVI

Dimensions - 1.61 x 1.34 x 4.6 inches;

68 grams (without battery)



Contemporary [redacted] 40

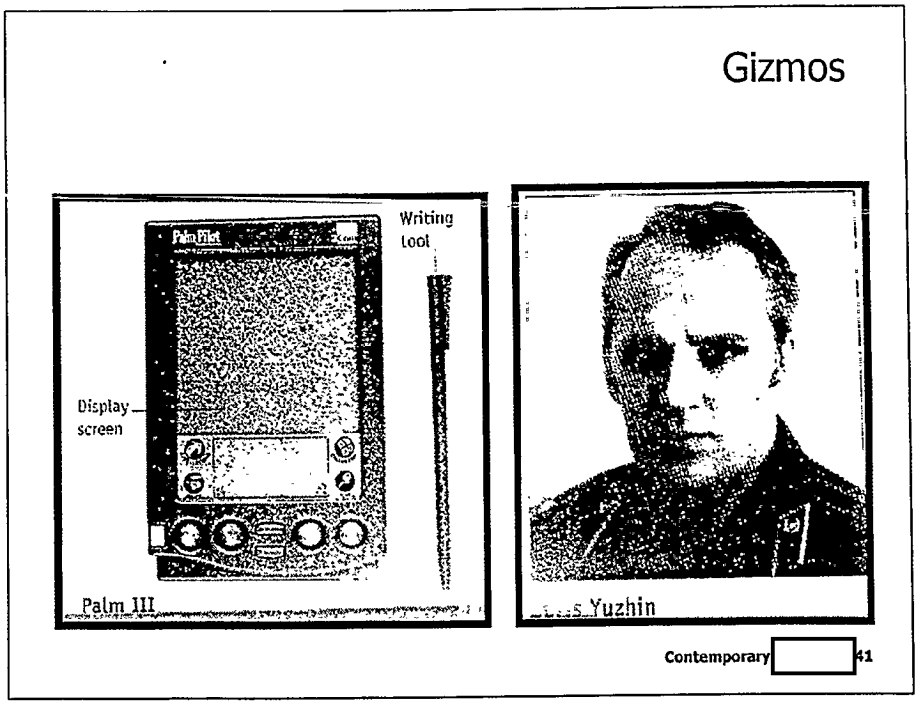
b7E

Teaching Points

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

See slide.



b7E

Teaching Point

Agents can innovate and create their own techniques to communicate sensitive intelligence.

Comment

Robert Hanssen, who compromised a number of CIA and FBI recruitments and used the FBI computer system to determine if he was being investigated, wrote a letter to his Russian handlers that was reprinted in an FBI affidavit. In it Hanssen proposed that, rather than bother with risky rendezvous in the muddy woods, he just send Moscow encrypted stolen documents via his Palm pilot (he wanted to upgrade from a Palm III to a Palm VII). Hanssen made it clear he wanted to be of greater help. He told the Russians that he needed a faster and more secure means of communicating with them, perhaps with a new Palm VII organizer with wireless Internet capability. If he had a faster way to contact the Russians, the letter states, he might have been able to warn Moscow that a listening device had been found at the State Department. "Such matters are why I need rapid communications...It can save you much grief."

The human side of all this is illustrated by Boris Yuzhin, a KGB officer who was recruited by the FBI. Yuzhin was arrested and held prison in Moscow and his FBI handler, SA Larry Williams, in SF thought he had been executed. Yuzhin was released after the wall fell and was interviewed by a CNN TV crew in Moscow at the time of the demonstrations in front of the Russian Parliament Building. CNN had been looking for a Russian who spoke English and found Yuzhin. Larry saw the interview, shouted "he's alive," and arranged for Boris to come to the US. Boris is now happily retired in SF where he lives on a GM-14 pension.

Countering the Cyber Threat

- Graphical Passwords
- Biometric Passwords
- Secure Coding
- Encryption
- Identifying Vulnerabilities
- Comprehensive Proprietary Information Protection Program

Contemporary [redacted] 42

b7E per FBI

Teaching Point

There are various methods by which we can counter the cyber threat.

Comment

See slide and describe each of the capabilities listed.

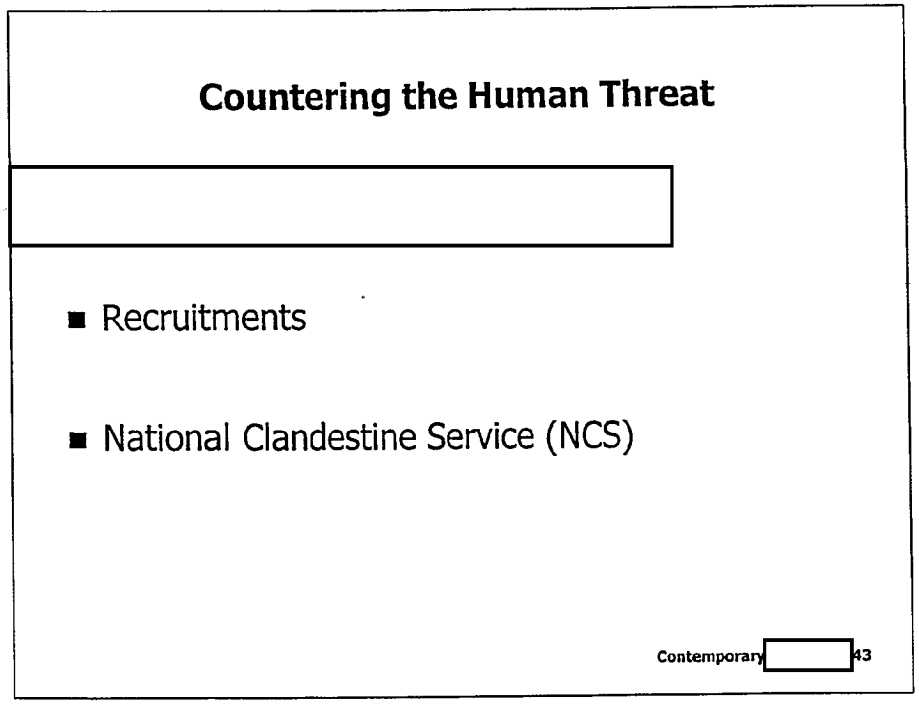
b1 per FBI
b7E

Note a weakness is that we can have procedures and rules and fail to follow them. For example, [redacted]

(S) [redacted]

Referral/Direct

ACLURM032068



b1
b7E

Countering the Human Threat is this all there is?

Countering the Human Threat

(S) [redacted]

b1
b7E

Pitts

Lessenthien

Trofimov

Contemporary [redacted] 44

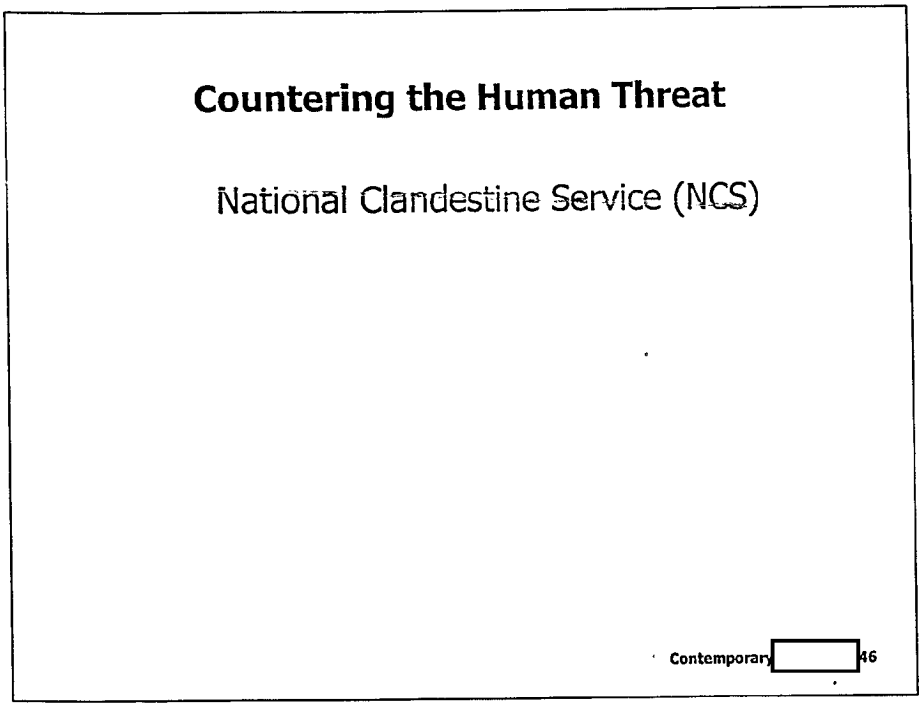
Countering the Human Threat

Recruitments

Contemporary [redacted] 45

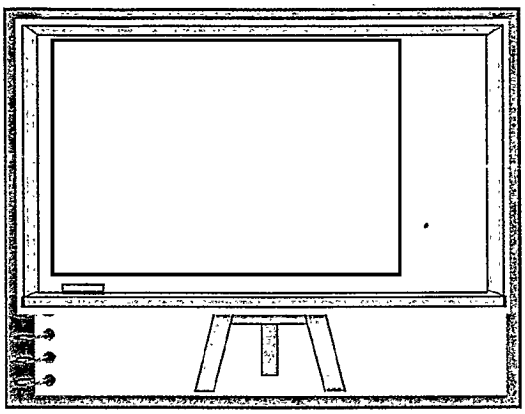
(S) Discuss the benefits of recruitment i.e. Hanssen [redacted]

b1
b7E



b7E

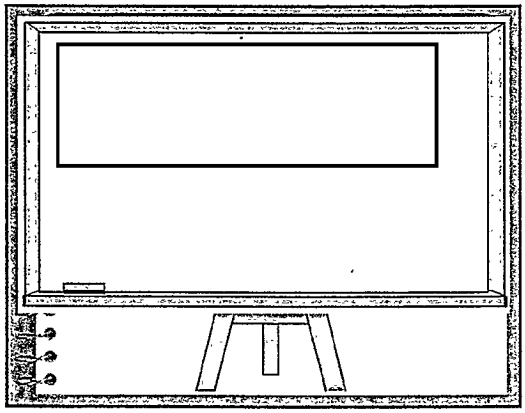
The new entity will oversee human intelligence operations conducted by the 15 U.S. agencies involved in spying, including the FBI and the Defense Intelligence Agency, a branch of the Pentagon. "This is another positive step in building an intelligence community that is more unified, coordinated and effective, and is better positioned to meet the increasingly complex intelligence challenges of the future," said John D. Negroponte, director of national intelligence. "The NCS will serve as the national authority for the integration, coordination, de-confliction and evaluation of human intelligence operations across the entire intelligence community," Negroponte said in a news release.



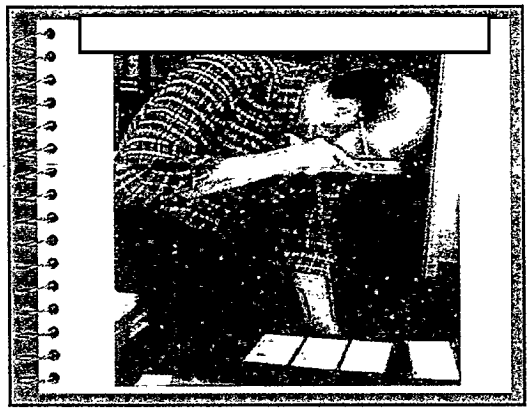
b7E



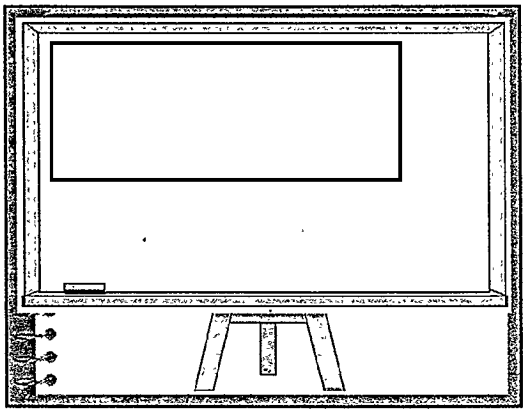
b7E



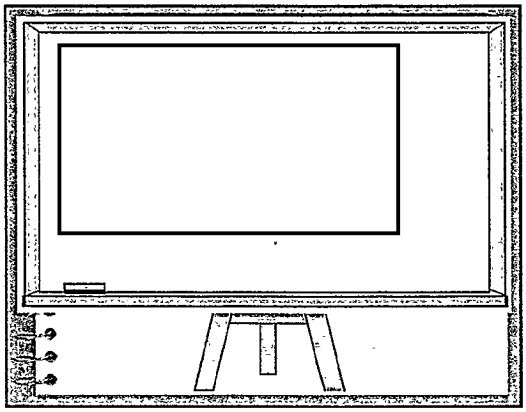
b7E



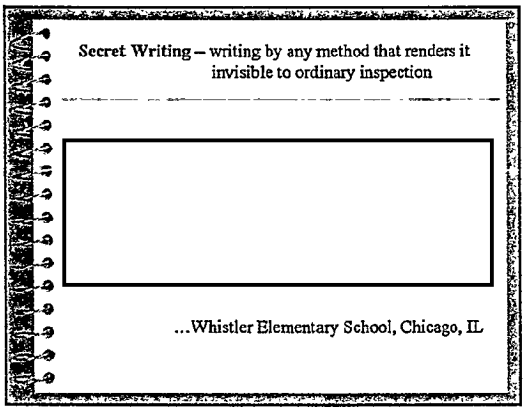
b7E



b7E

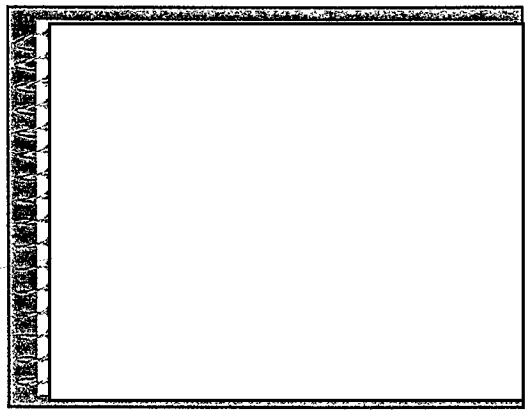


b7E



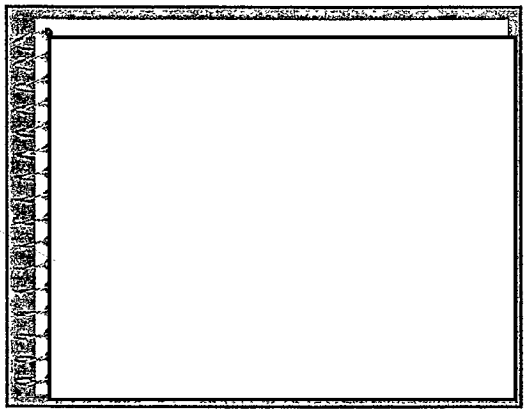
b7E

(S)



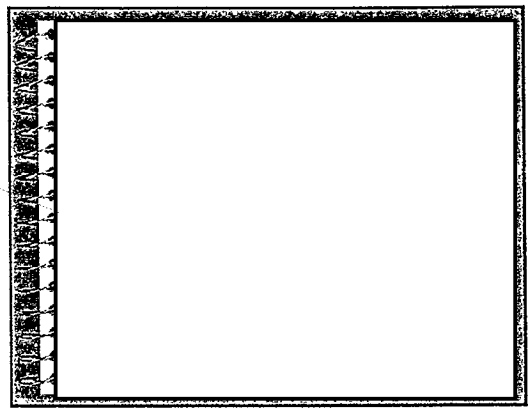
b1
b7E

(S)

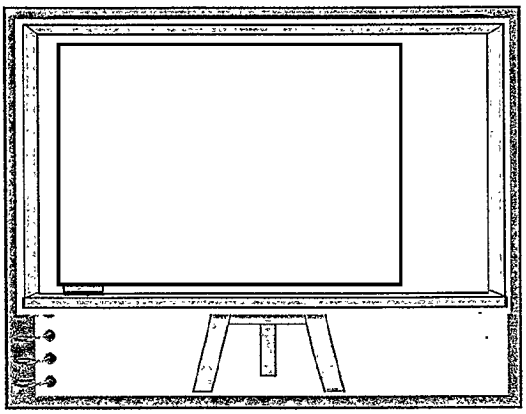


b1
b7E

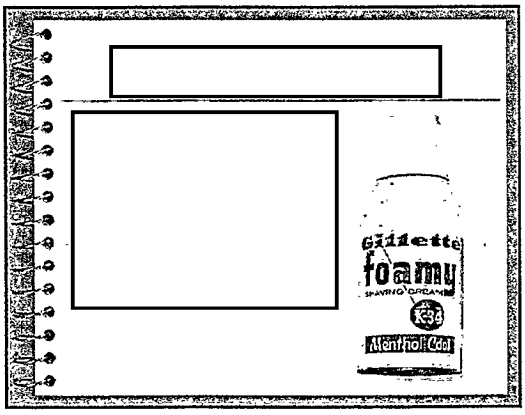
(S)



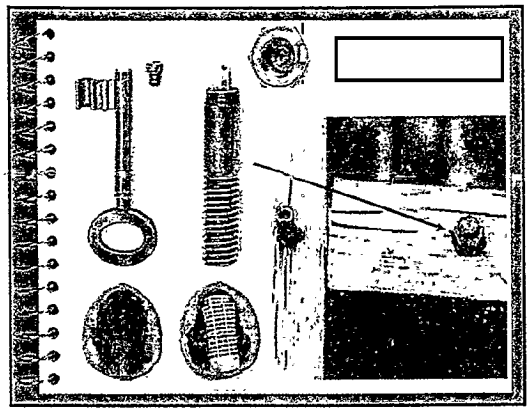
b1
b7E



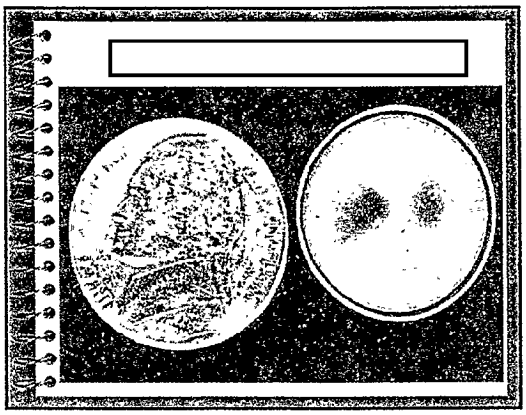
b7E



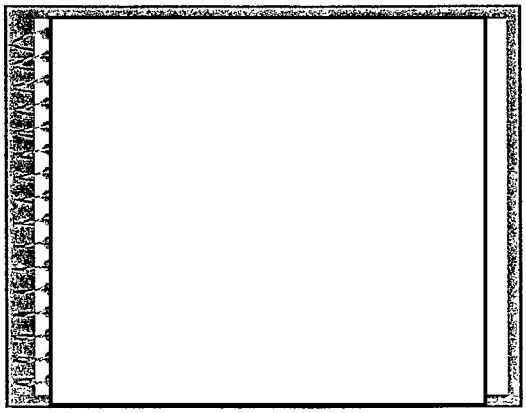
b7E



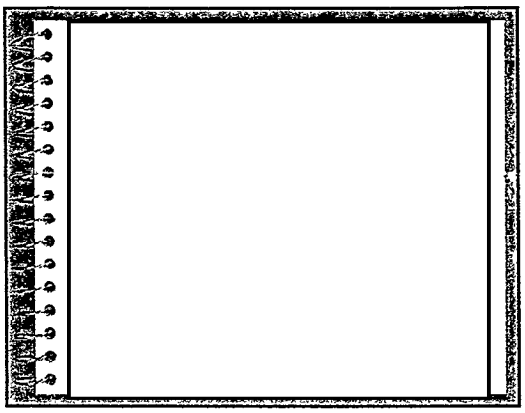
b7E



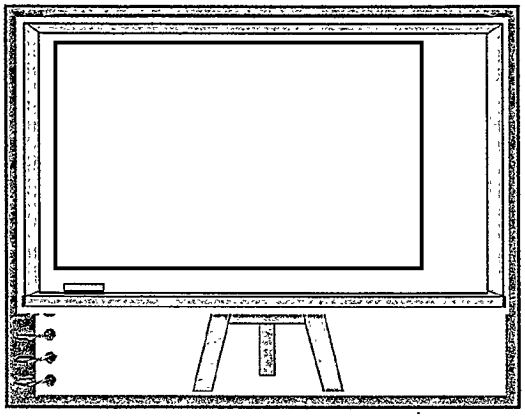
b7E



b7E

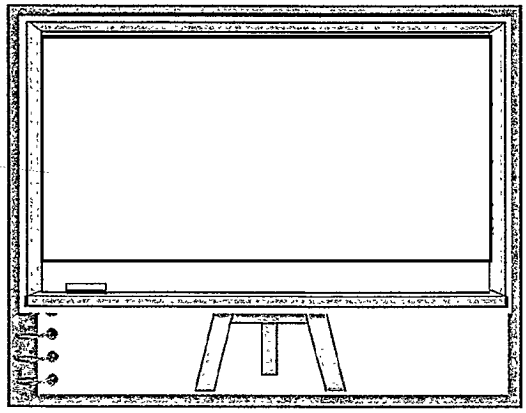


b7E



b7E

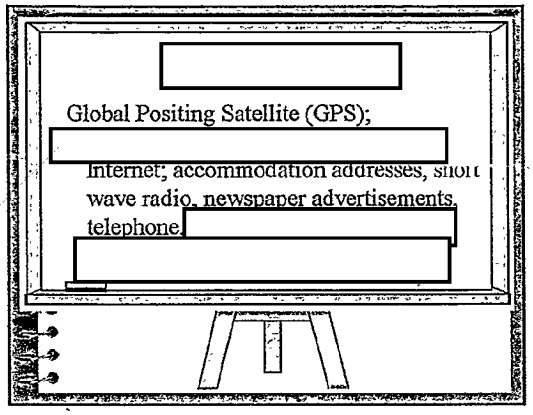
(S)



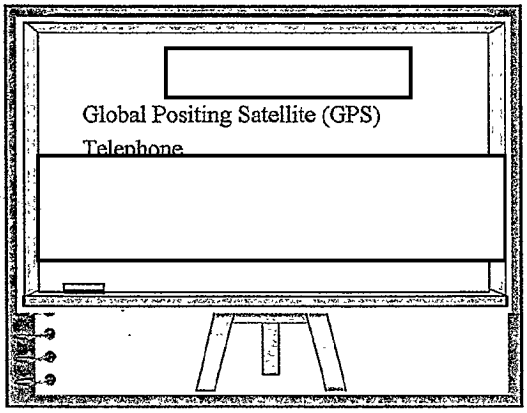
b1
b7E

b1
b7E

(S)

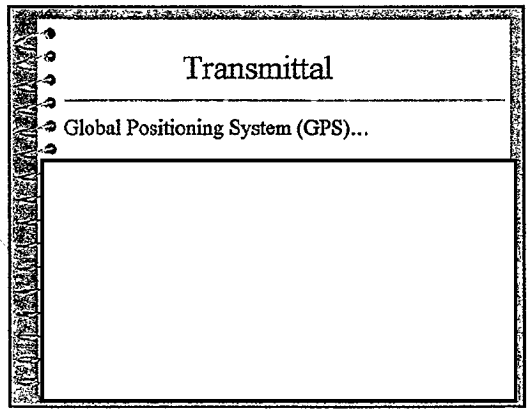


(S)



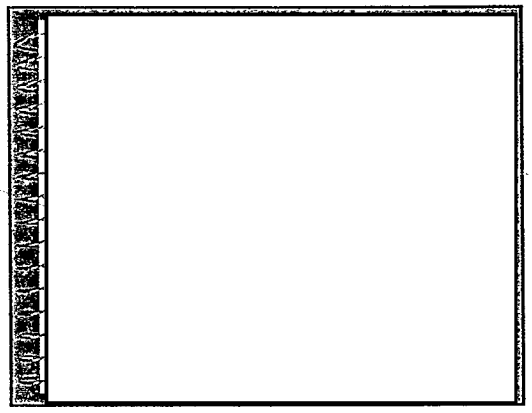
b1
b7E

(S)



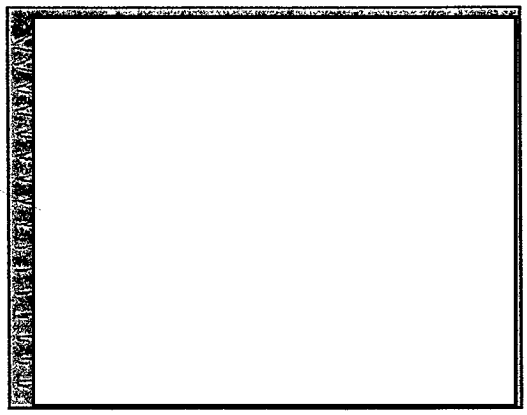
b1
b7E

(S)



b1
b7E

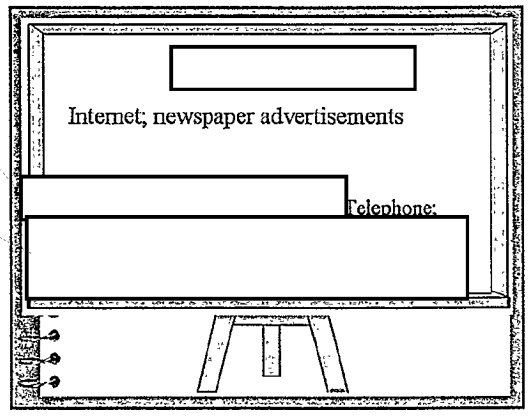
(S)



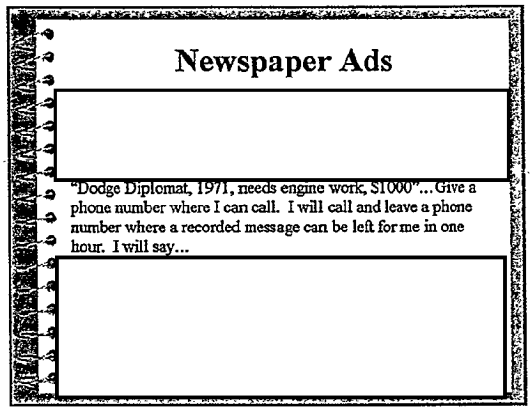
b1
b7E

(S)

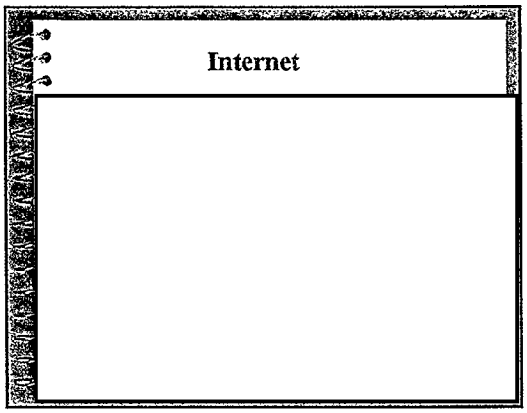
(S)



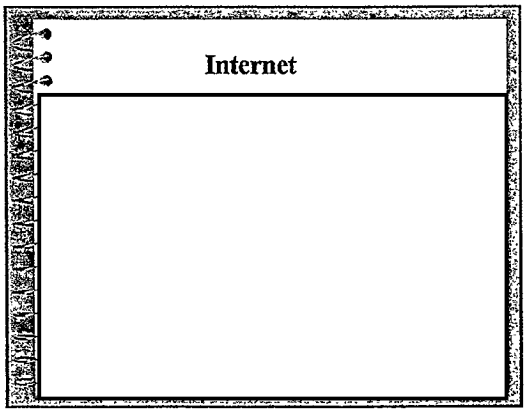
b1
b7E


Newspaper Ads
"Dodge Diplomat, 1971, needs engine work, $1000"... Give a phone number where I can call. I will call and leave a phone number where a recorded message can be left for me in one hour. I will say...

b7E

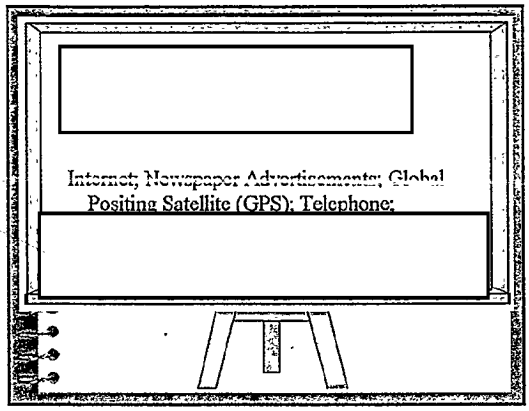

Internet

b7E


Internet

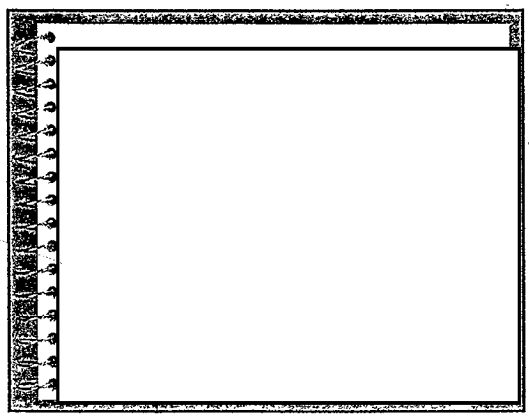
b7E

(S)

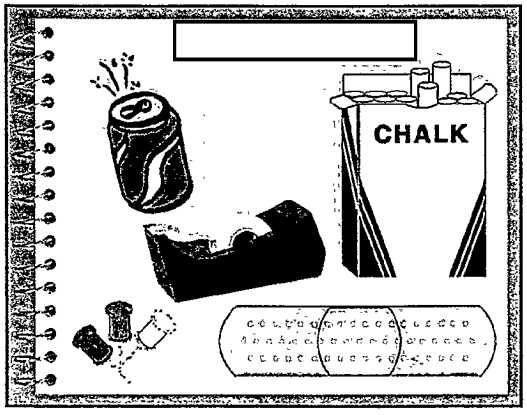


b1
b7E

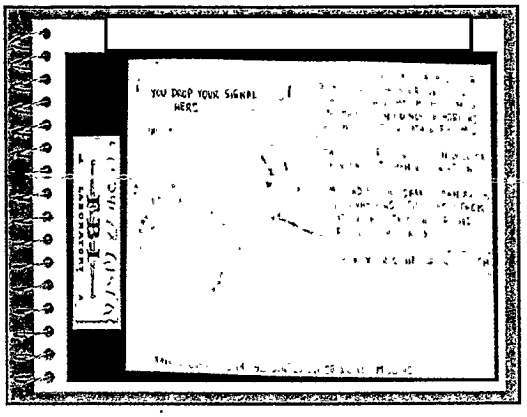
(S)



b1
b7E

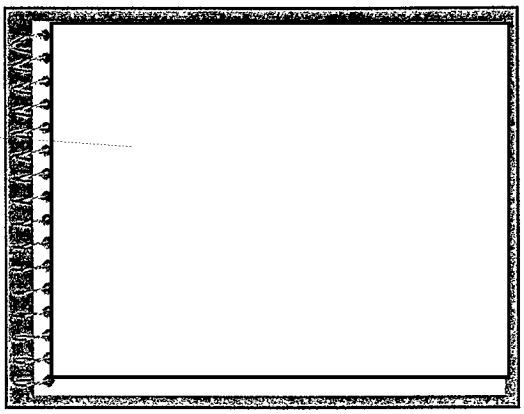


b7E

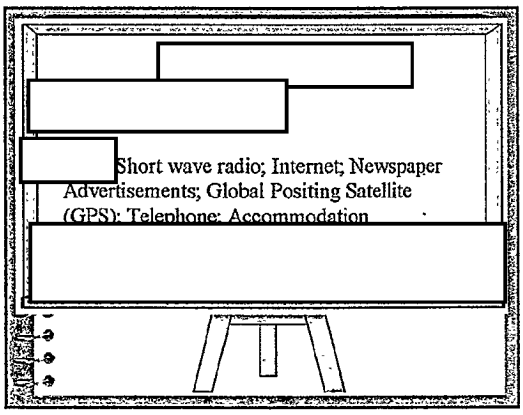


b7E

(S)

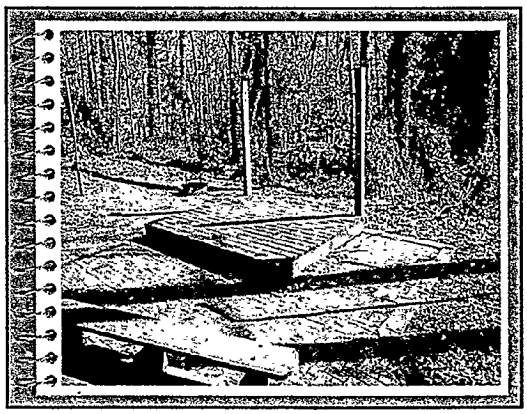


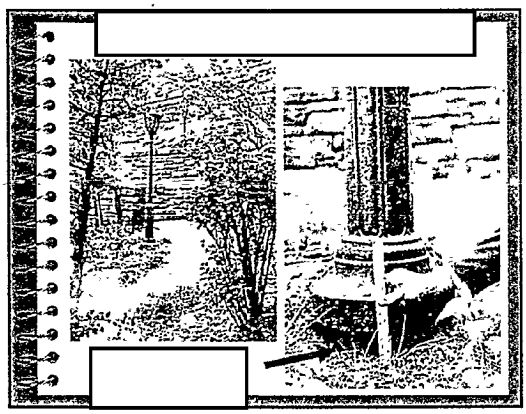
b1
b7E



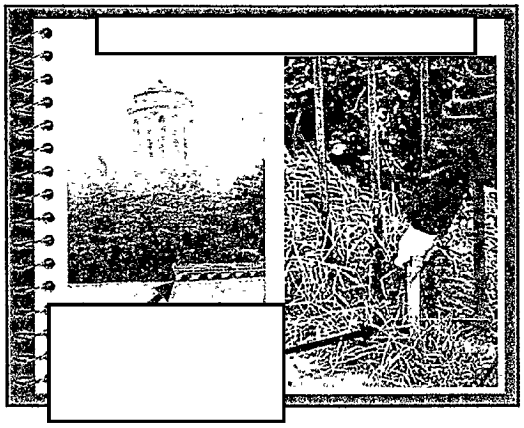
b1
b7E

b7E

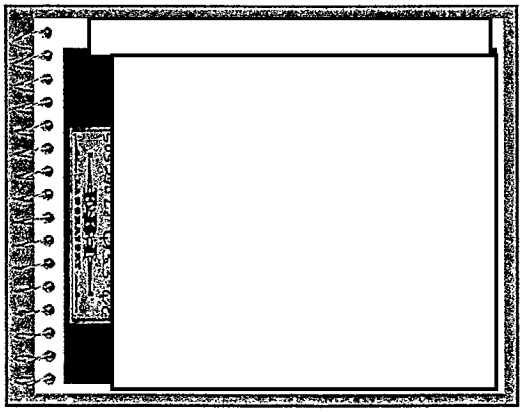




b7E



b7E



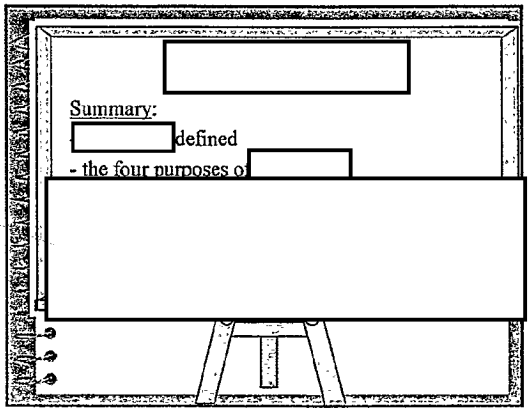
b7E



b7E

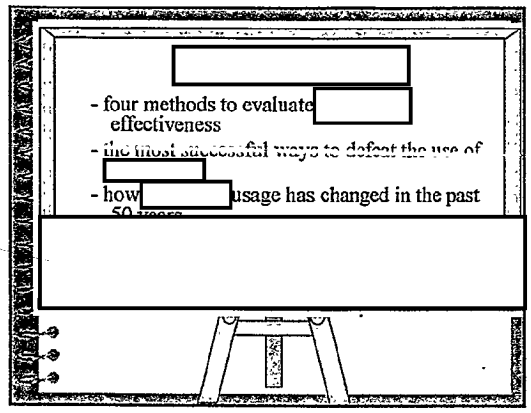


b7E



(S)

b1
b7E


- four methods to evaluate effectiveness
- how usage has changed in the past

(S)

b1
b7E


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

DATE: 01-09-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Federal Bureau of Investigation
Counterintelligence Training Center

Lesson plan for [redacted]

b1
b6
b7C
b7E

Title: [redacted]

(S) Length of lesson: 2 hours
Target Audience: New agents, analysts, surveillance teams [redacted] and intelligence community members with little or no experience in Counterintelligence [redacted]

Instructor: SSA [redacted]

Instructional Methods Used:

Exercise in [redacted]

(S) Lecture from PowerPoint

Exercise in planning [redacted]

b1
b7E

Exercise in defeating opponents' [redacted] on paper.

Date prepared: 09/27/2004

Additional information: Lesson plan can be lengthened by an hour if students are provided maps and instructional exercise to develop a

(S) [redacted] is planned in groups of no more than four.

Statement of Goals and Objectives

Goal:

Familiarize the audience with [redacted] terminology and usage by Intelligence Officers. b7E

Objectives:

At the end of this 2-hour block of instruction, students will be able to:

- define [redacted]

- list four purposes of [redacted]

- list the four methods of evaluating the effectiveness of [redacted]

(S) [redacted] b1 b7E

- list the three most successful ways to defeat the use of [redacted]

- explain how [redacted] usage has changed in the past 50 years.

(S) - assess how the change in [redacted] usage [redacted] b1 b7E

Equipment Requirements

Equipment for Instructor

Computer with Microsoft PowerPoint installed or a PowerPoint reader

Easel with pad or white board

Fat magic markers or Dry Erase markers

Projector for computer

Projection Screen

PowerPoint Slide presentation entitled [redacted]

Work to be done prior to class entering room [redacted]

[redacted] b7E

Equipment for Students

Pens or pencils

Notepads

PowerPoint handout; three slides to each page

(S) (Option for additional hour of instruction for exercise: Copies each, for students, of an identical street map or a portion of a local street map. Maps must have enough clarity for the students to [redacted] b1 b7E

Lesson Plan

	Introduction of self and topic Goal: Familiarize the audience with [redacted] terminology and usage by Intelligence Officers. Objectives: At the end of this 2-hour block of instruction, students will be able to: - define [redacted] - list four purposes of [redacted]	Slide #1
(S)	[redacted]	
	- list the four methods of evaluating the effectiveness of [redacted] - list the three most successful ways to defeat the use of [redacted] - explain how [redacted] usage has changed in the past 50 years.	
(S)	- assess how the change in [redacted] usage [redacted]	
		Slide #2, 3 Make sure audience is familiar with terms [redacted]
	(Objective #1)	Slide #4
(S)	Define [redacted]	Discuss with students the similarities between [redacted] usage [redacted]
		Go over each element of definition: [redacted]

b1
b7E

b1
b7E

	Service Mission Clandestine
(Objective #2 – List four purposes of [redacted]) Purposes:	Slide #5
(S) [redacted] (S) [redacted] (S) [redacted]	b1 b7E
(Objective #3 List for methods of evaluating the effectiveness of [redacted])	Slides #6 to #14 Photographs
(S) [redacted]	b1 b7E Ask student to take out list of [redacted] found in room. Evaluate each [redacted] used to see how it meets these four criteria.

[redacted] is the best example of this.

Compare the list of four evaluating factors with which ways can best be defeated. [redacted]

(S) So how do you defeat good [redacted]

b1
b7E

[redacted]

(Objective #4 Ways in which [redacted]

Slides #15 to #20

Explained that each will be detailed in the following slides.

[redacted]

Slides #21 to #25

(S)

b1
b7E

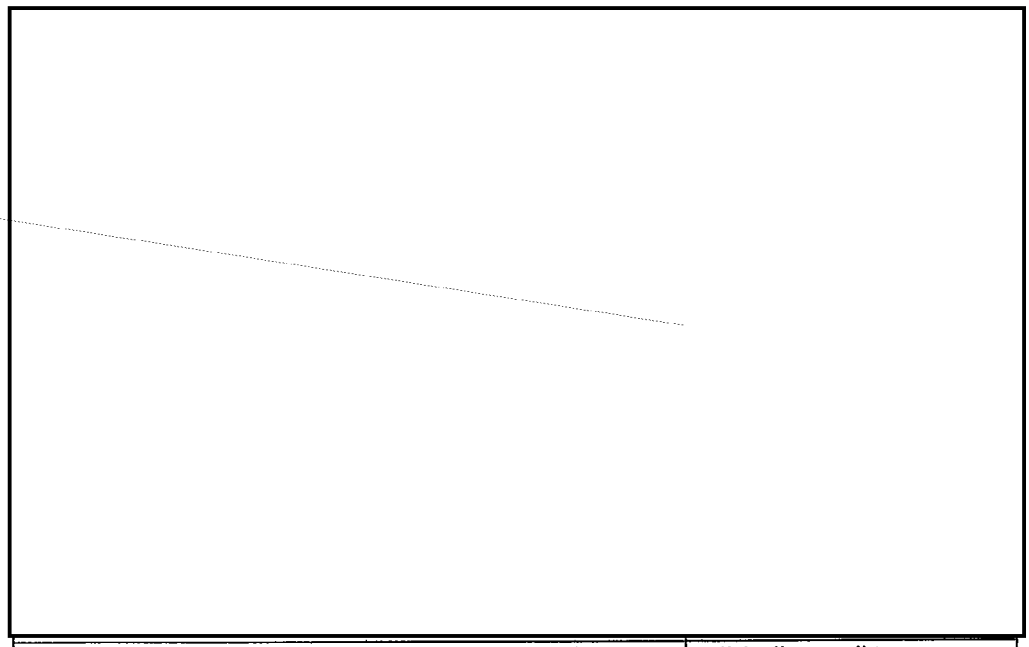
Example: 1995 –Michael Stephen Schwartz, US Naval Commander charged with passing DOD classified documents on classified diskettes to Saudi naval officers from 1992 to 1994 while assigned in Riyadh. He was charge with four counts of espionage and five counts of removing classified materials to his home. In a plea he received an "other than honorable" discharge and lost all retirement and military benefits. The Virginian-Pilot (Nofolk, VA, May 25, October 14, 1995; Washington Post, September 13, 1995.)

(S)

b1
b7E

(S)	b1 b7E
The Sword and The Shield, pg 141-142. (1999, Basic Books, Inc.);	
Show video of cue the tape to the segment on	
Concealment Devices An innocuous object designed or adapted as a container for hiding material or equipment (money, film, documents, cameras, radios, etc)	Slides #25 to #32
(S) (Objective #5 Describe ten types of discussed in which stolen information is transmitted	Slides #33 to #38 GPS note - Robert Hanssen had purchased a GPS shortly before his arrest. Telephone note - Anna Montes, who spied for Cuba, had a
(S) 1. Global Positing Satellite (GPS); 2. (S) 3. Internet; 4 5. short wave radio, (S) 6. newspaper advertisements, 7. telephone,	b1 b7E

(S)



b1
b7E

(slides on Internet; newspaper advertisements)	Slide #39 to #42
(slides on [redacted] Short wave radio)	Slide #43 to #47 Anna Montes used short wave radio to communicate with Cuba
	Slides #48 to #56

(S)

b1
b7E

each other. The package is disguised to conceal its contents.

Example:

(S) Brush pass:

b1
b7E

Example: 1996 Robert C. Kim, Office of Naval Intelligence. A civilian who was arrested outside a diplomatic reception at Ft. Myers, Virginia as he stood beside Capt. Baek Dong -11 of Korean Embassy Naval Attaché. Kin was a native of Korea who became a citizen and passed dozens of classified, some TS, and documents to Baek. Convicted of conspiracy to commit espionage. Washington Post, Sept 26, 1996, Oct. 2, 1996, LA Times May 8, 1997.

(S) (Objective # 6. List the three most successful ways to defeat the use of)

(Objective #7 – Explain how has changed in the last 50 years)

b1
b7E

(S) (Objective #8 – Assess how changes in usage over the past 50 years

(S) Discuss how usage has changed in the past 50 years. Discuss the change in usage Make two observations about the changes in Note that the type of has increased, and the method of

transferring materials has become more sophisticated and, arguably, easier, with the onset of the Internet and digital means.

For example, [redacted] in the last 50 years has changed in a cumulative way. The methods of stealing secrets from 50 and even 100 years ago are still in use; however, new methods have been added to the spies' toolboxes. In years past, a spy was limited to the bulk of film or the mechanics (tools and time) of reducing film to a microdot. The alternative was to transfer massive amounts of bulky paper. Today, digital scanning and transference permits a spy to amass and transfer large amounts of material for espionage in very small packages. For example, all the materials stolen by the [redacted]

b7E

In addition, the methods of transference of stolen materials have changed. The use of the [redacted]

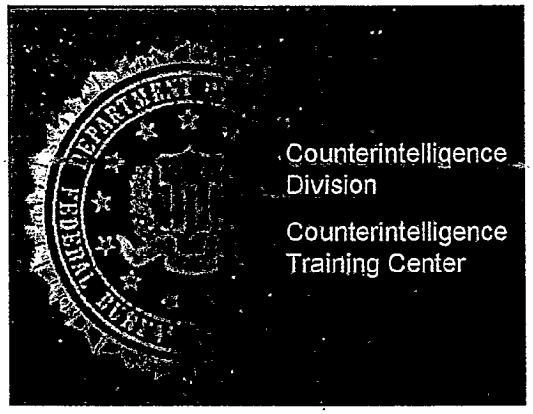
(S) Assess how the change in [redacted] usage over the past 50 years [redacted] One example of changes in [redacted] and the way law enforcement can seek to defeat these changes [redacted]

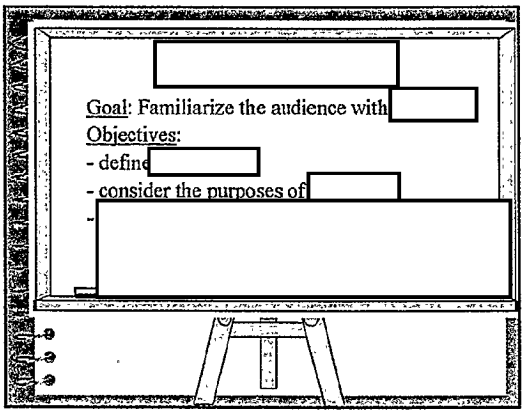
b1
b7E

[redacted] Counterintelligence investigators must seek to update their arsenal through continual training to be aware of methods used by spies. Counterintelligence investigators must [redacted]	b7E
	Discuss how the [redacted] marked in the room at the beginning of the class is obvious if you are looking for [redacted] Ask the class what they think are some of the most effective [redacted]
What have we accomplished? Now you should be able to: - define [redacted] - list four purposes of [redacted] - describe five ways [redacted] is stolen,	
(S) [redacted]	b1 b7E
- list the four methods of evaluating the effectiveness of [redacted]. - list the three most successful ways to defeat the use of [redacted] - explain how [redacted] usage has changed in the past 50 years. - assess how the change in [redacted] usage [redacted]	Remember to ask if there are any questions. (Remove [redacted] in room.)

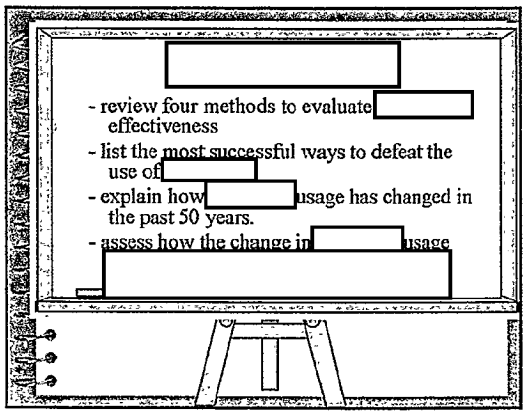
DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



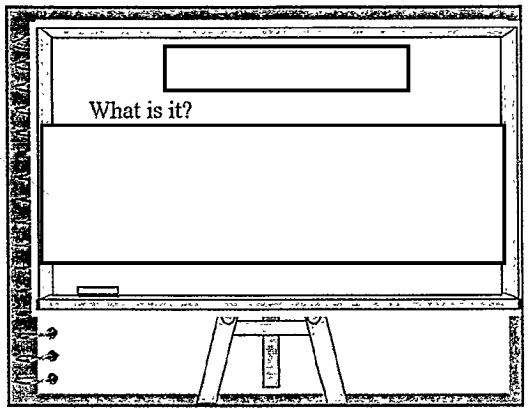


b7E



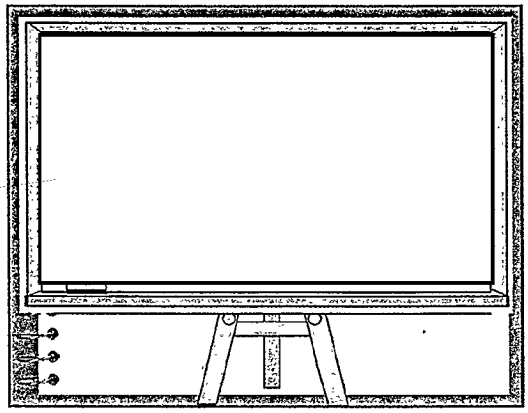
b7E

(S)

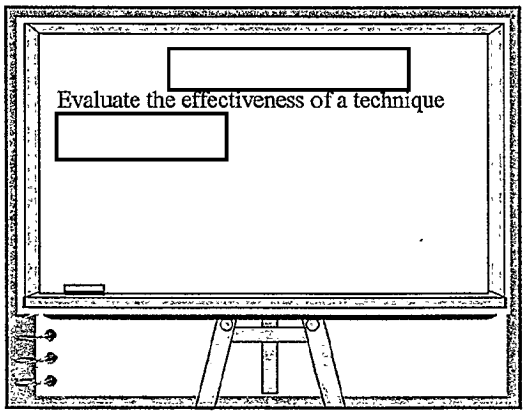


b1
b7E

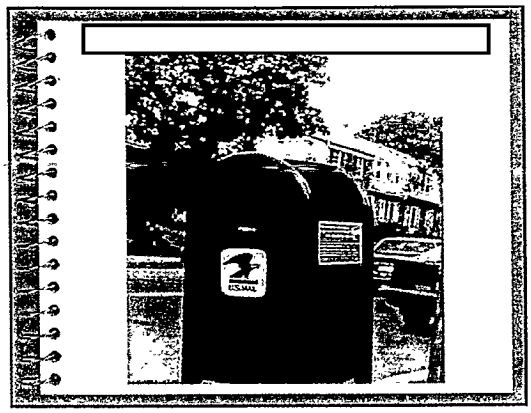
(S)



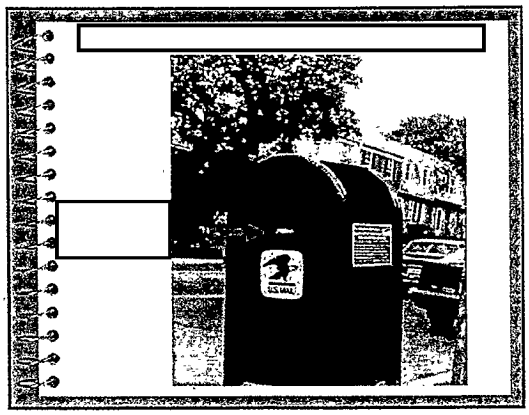
b1
b7E



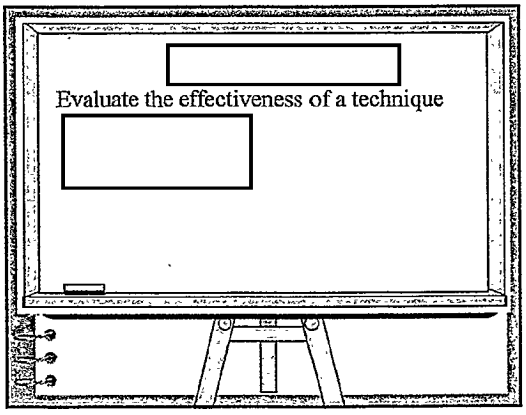
b7E



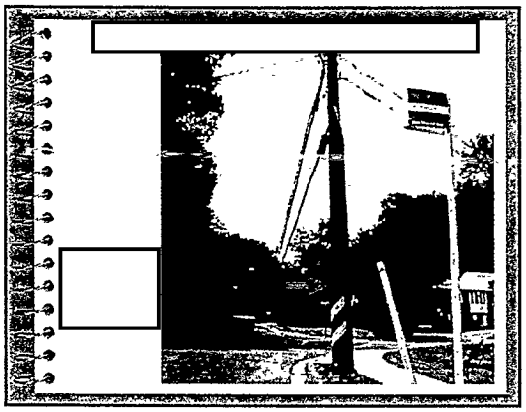
b7E



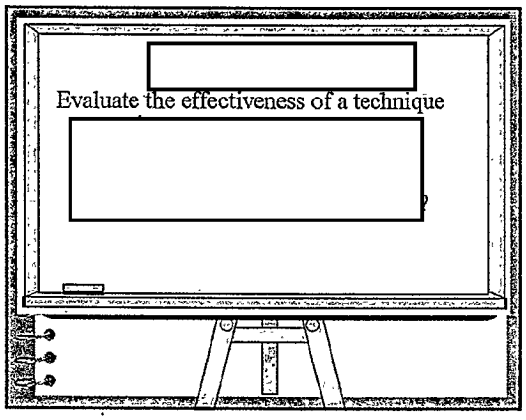
b7E



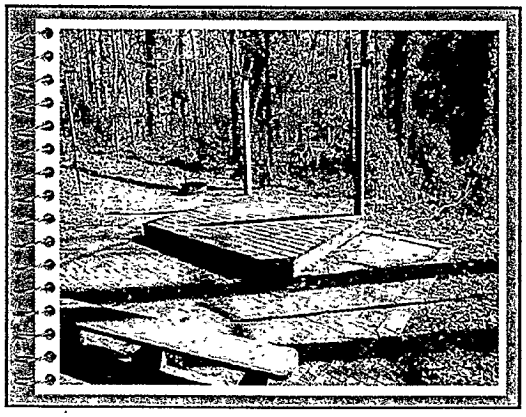
b7E

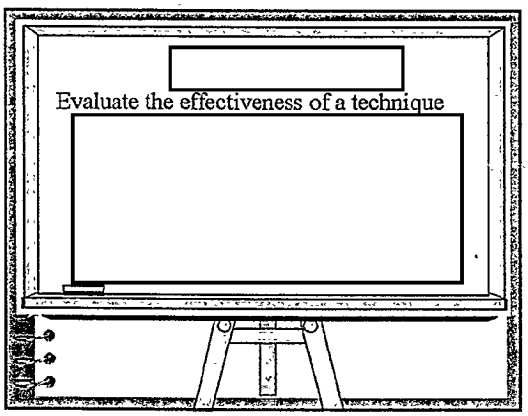


b7E

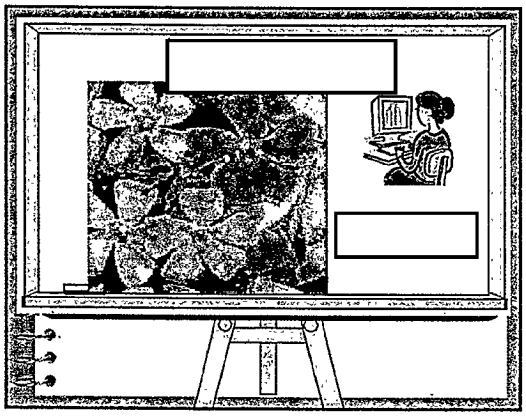


b7E

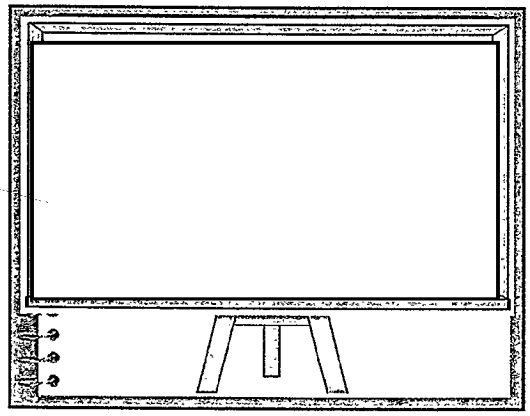




b7E



b7E



(S)

b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

THE GAME ON THE STREET

(S)

b1
b7E

WHO AM I?

(S)

b1
b7E

MY GOALS TODAY:

(S)

b1
b7E

~~SECRET~~

GROUND RULES:

(S)

b1
b7E

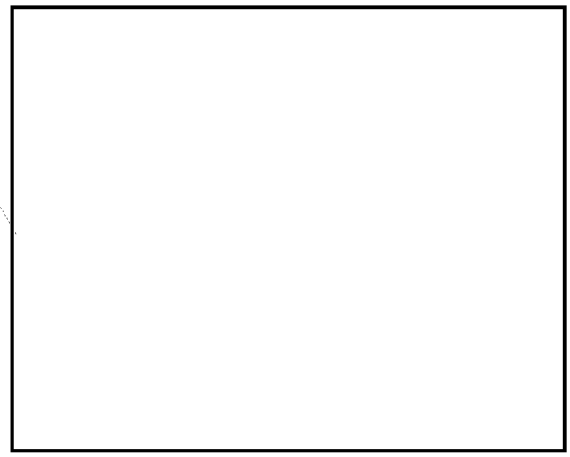
(S)

b1
b7E

(S)

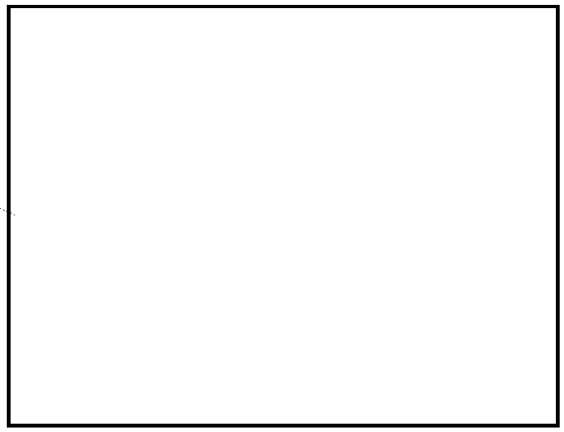
b1
b7E

(S)



b1
b7E

(S)



b1
b7E

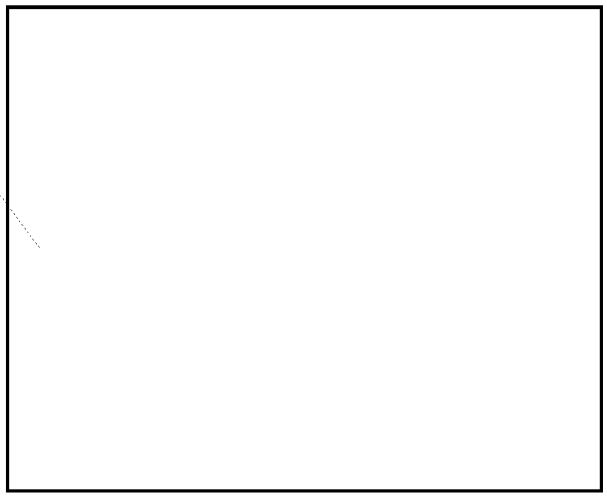
LET'S LOOK AT SOME

(S)



b1
b7E

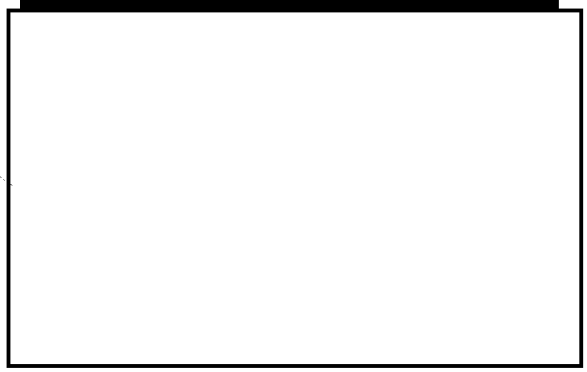
(S)



b1
b7E

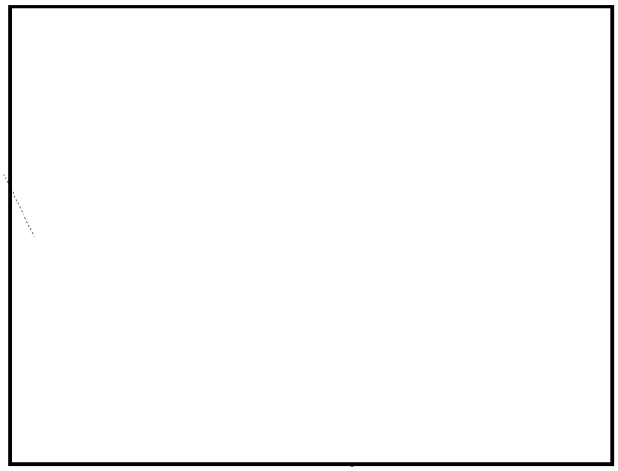
I MIGHT DO THIS:

(S)



b1
b7E

(S)



b1
b7E

I MIGHT TRY THIS:

(S)

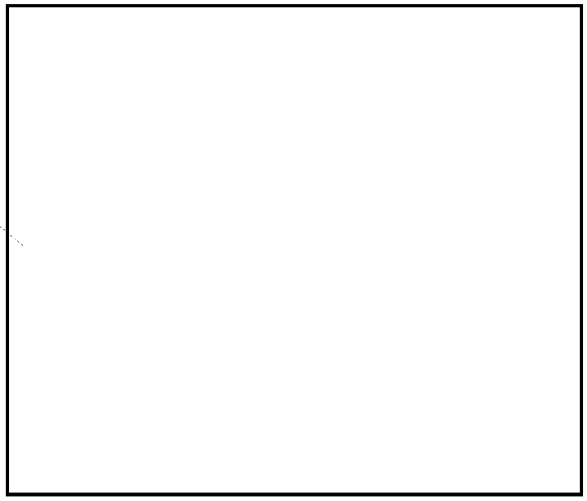
b1
b7E

(S)

b1
b7E

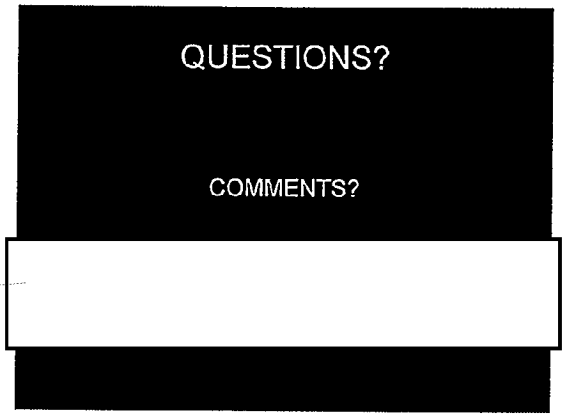
(S)

b1
b7E



(S)

b1
b7E



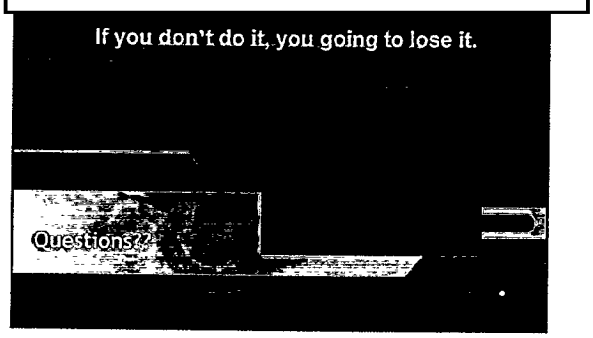
(S)

b1
b7E

(S)

b1
b7E

(S)



b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b6
b7C
b7E



CIOPs



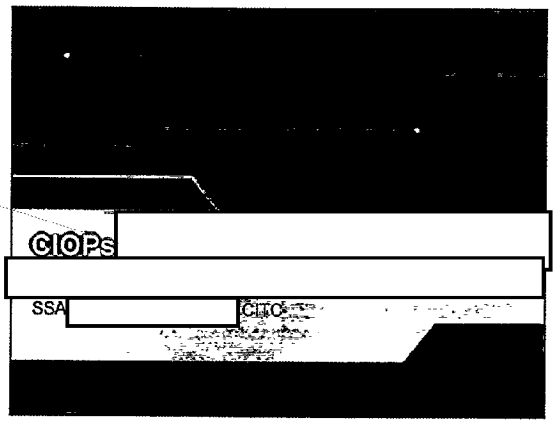
(S)

(S)

Proprietary
Prepared By: SSA

~~SECRET~~

(S)



b1
b6
b7C
b7E

(S)

b1
b7E

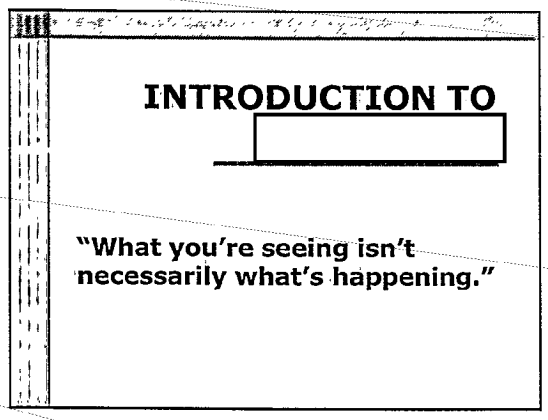
(S)

b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



(S)

(S)

b1
b7E

(S)

(S)

(S)

(S)

(S)

(S)

(S)

b1
b7E

(S)

(S)

(S)

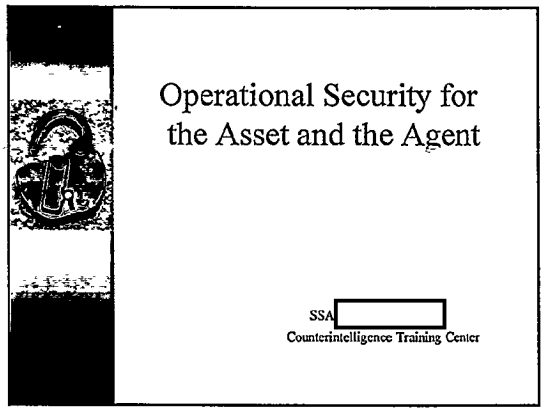
(S)

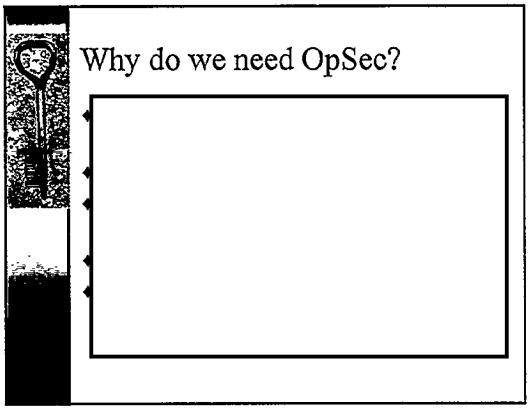
- Miscellaneous

b1
b7E

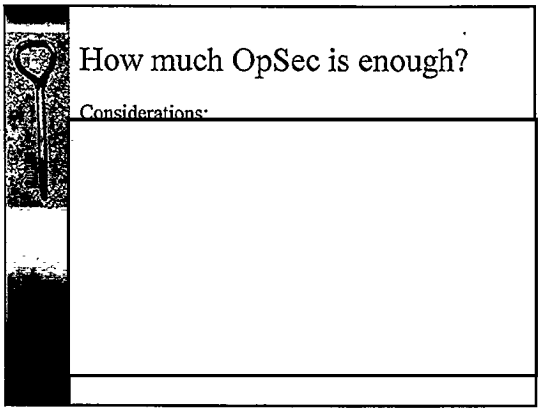
DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

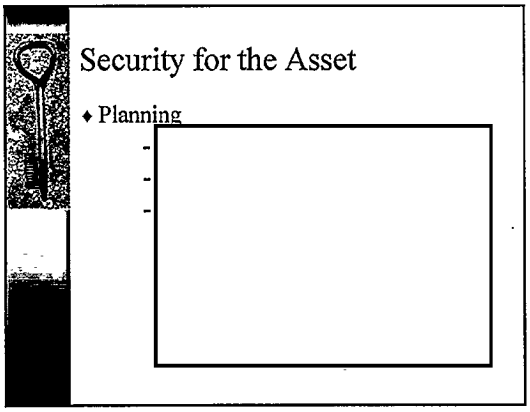




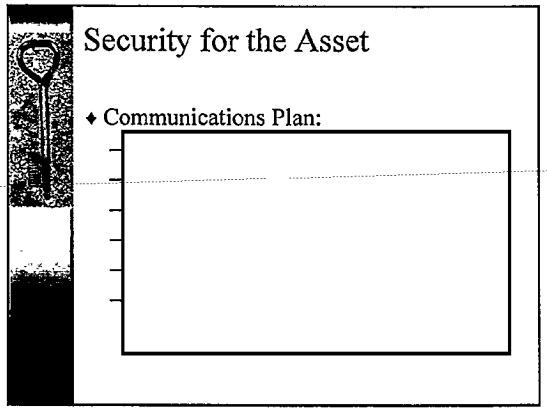
b6
b7C
b7E



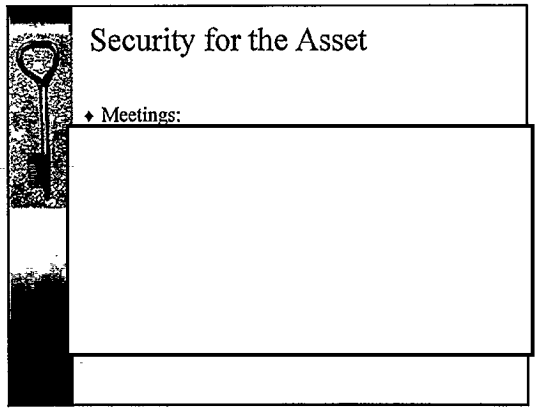
(S)



b1
b7E



(S)



b1
b7E

Security for the Asset

- Information handling security:

(S)

Security for the Asset

- Emergencies:

b1
b7E

Security for the Asset

Some tools for the trade:

(S)

Security for the Special Agent

b1
b7E

Security for the FBI and USG

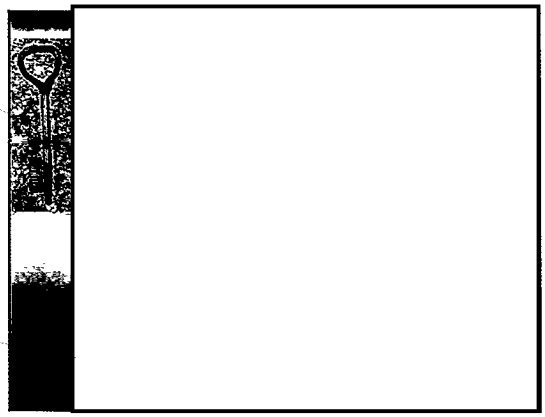
- What are you giving away? Communication is not always a two-way street!

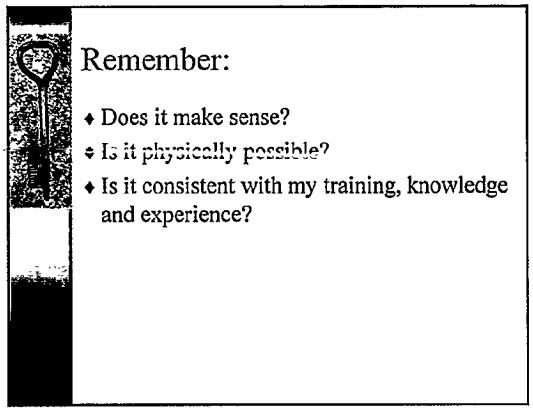
Reviewing Asset Performance

b7E

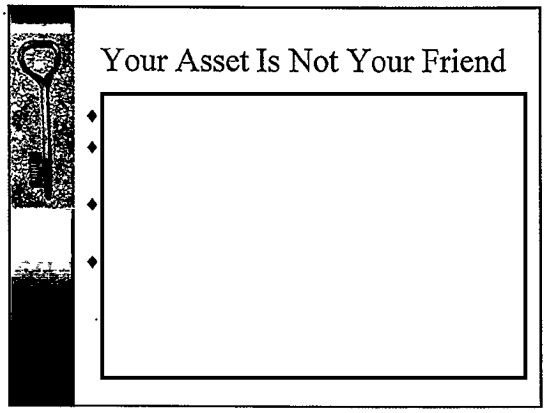
(S)

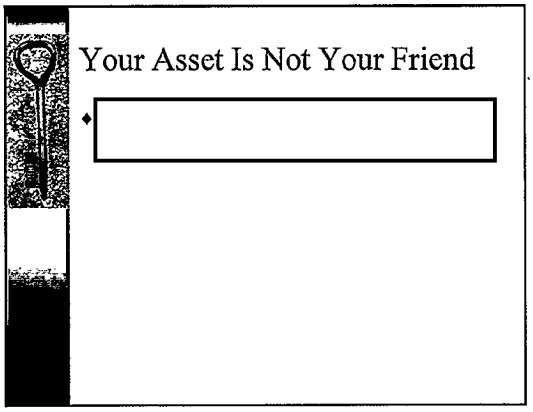
(S)



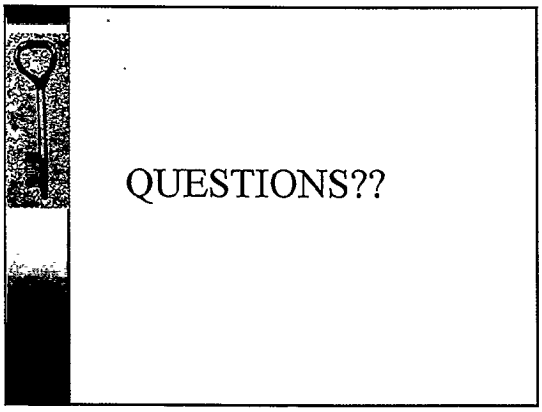

Remember:
♦ Does it make sense?
♦ Is it physically possible?
♦ Is it consistent with my training, knowledge and experience?

b1
b7E


Your Asset Is Not Your Friend


Your Asset Is Not Your Friend

b7E


QUESTIONS??

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

Outline of Activities

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Content Outline/Activities	Instructor Notes
(S) Introduction Thus far in this portion of the training course, you have been afforded a few hours of training regarding [redacted]. Included in this [redacted] **training** have been discussions regarding:	Slide #1 [redacted]
(S) [redacted]	b1 b7E
(S) [redacted]	Slide #2 [redacted]
(S) [redacted]	b1 b7E

copy

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
(S)	
(S)	
(S)	
(S)	

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	b1 b7E
(S) **Personnel Problems:**	Slide #3
	b1 b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
(S)	
(S)	

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
(S)	

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
(S)	
(S)	
(S)	

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
(S)	
(S)	

b1
b7E

(S) **Outline of Activities** 8

Content Outline/Activities	Instructor Notes

(S)

(S)

(S)

(S)

(S)

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	
Final Thoughts:	Slide #6 "Final Thoughts"
(S)	
At this point the instructor should allow for questions.	

b1
b7E

b1
b7E

~~SECRET~~

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/EAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Lesson Plan

(S) [redacted] b1 b7E

Lesson Length:	One Hour
Prepared By:	SSA [redacted] b6 b7C
Methods Used:	Lecture; Classroom Discussion
Preparation Date:	February, 2006
Target Learner Group:	Basic Counterintelligence Operations (CIOPs)

ACLURM032127

FBI031647

Items and Materials

Items/Materials to Teach the Class:

1. Power point projector
2. CD of presentation

Items/Materials for Each Student:

1. Handouts of presentation

Outline of Activities

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

	Content Outline/Activities	Instructor Notes
(S)		Slide #1
	Introduction	
(S)	Earlier, we discussed the concepts of	b1 b7E
(S)		Slide #2
		b1 b7E
(S)		
(S)		

Outline of Activities

Content Outline/Activities	Instructor Notes
Other Considerations: **Get away from the vehicle:**	Slide #3 "Other Considerations"
(S) [redacted]	
(S) [redacted]	
(S) [redacted]	Slide #4 [redacted]
(S) [redacted]	

b1
b7E

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
Compass and Maps:	
(S)	
Paper and writing utensils:	
(S)	
Disguise:	
(S)	
Food and Water:	
(S)	
(S)	Slide #5
(S)	

b1
b7E

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	Slide #6
(S)	b1 b7E
(S)	Slide #7
(S)	
(S)	b1 b7E
(S)	
(S)	Slide #8
(S)	This requires no personal contact. b1 b7E
(S)	
(S)	

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S)	Slide # 9
(S)	

b1
b7E

b1
b7E

Outline of Activities

(S)	Content Outline/Activities	Instructor Notes
		Slide #10
(S)		
(S)		Slide #11
(S)		

b1
b7E

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	Slide #12
(S)	b1 b7E
(S)	Slide #13
(S)	b1 b7E
May be difficult to develop cover for maintenance or repair activities.	

(S)

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	Slide #14
(S)	Slide #15
(S)	
(S)	

b1
b7E

b1
b7E

Outline of Activities

(S)

Content Outline/Activities	Instructor Notes
	Slide #16
(S)	
(S) At this time, questions may be fielded from the class. The display of the terms covered should stimulate classroom questions and discussion.	Slide #17

b1
b7E

b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Statement of Objectives

Instructional Goal:

(S) At the conclusion of this class, the student will be able to articulate the concept of

(S) The student will be able to conceive

b1
b7E

Instructional Objective:

At the conclusion of the class, the student will be able to:

(S)
1)
2)
3)

b1
b7E

~~SECRET~~

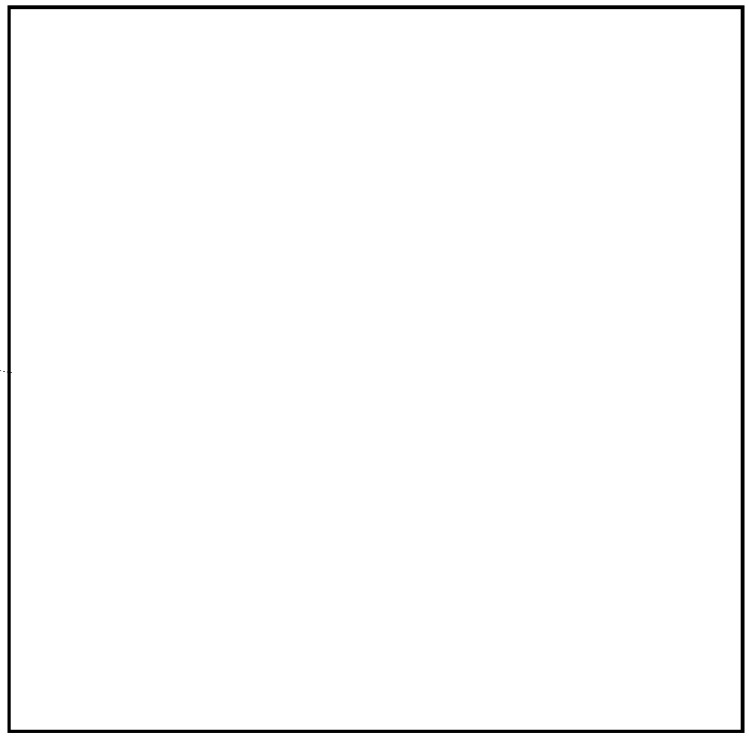
Test Answers

1.

2.

3.

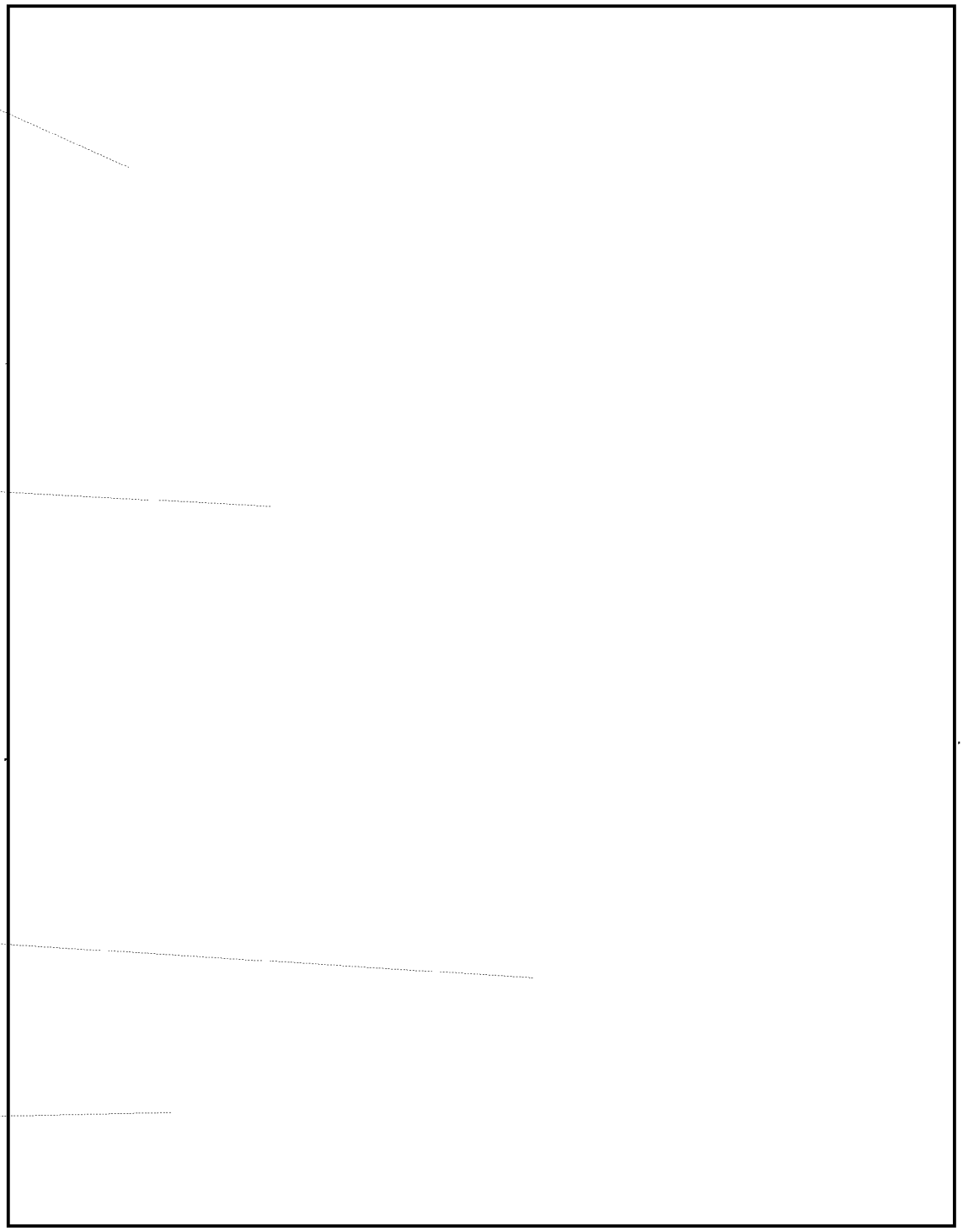
(S)



b1
b7E

4.

Test



(S)

(S)

(S)

(S)

b1
b7E

ACLURM032140
FBI031660

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-10-2012 BY 65179/DMH/BAW/STP/bls

Lesson Plan
"Introduction to [redacted]"

b7E

Lesson Length:	2 Hours
Prepared By:	SSA [redacted]
Methods Used:	Lecture, Discussion, Powerpoint
Preparation Date:	January, 2006
Target Learner Group:	Basic Counterintelligence Operations (CIOPs)

b6
b7C

Items and Materials

Items/Materials to Teach the Class:

1. Lesson CD
2. Powerpoint Projector
3. Screen (or blank wall)
4. Chalkboard and Chalk (or flipchart and markers)

Items/Materials for Each Student:

1. Powerpoint Presentation handouts (optional at instructor discretion)

ACLURM032142

FBI031662

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

Outline of Activities

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Content Outline/Activities	Instructor Notes
Introduction This block of instruction will concern [redacted]. We are going to discuss the ways [redacted] is utilized, why it is utilized, and why it is effective. Many of the methods we will discuss have been in use for a number of years, and while not "electronically" technical, or sophisticated nonetheless. [redacted] has been in use as long as [redacted]. The warrior king Sun Tzu authored his classic work, "The Art of War" in about 500 B.C. In this work-considered by many to be the definitive martial treatise-there is an entire chapter in this devoted to spying and intelligence gathering. [redacted] was a [redacted]	Slide #1 "Introduction To [redacted]" b7E
(S) "Everything has a definition"; This is how our adversaries conduct their activities and get their job done. [redacted]	Slide #2 [redacted] Definition b1 b7E
Our use of [redacted] assists us in the enforcement of **EO 12333**. -------**EO12333** provides the FBI with primacy in CI matters; **EO12333** signed in late 1940s------	Slide #3 "Why [redacted]"
(S) [redacted]	b1 b7E
(S) [redacted]	Slide #4 "Categories of Operational Acts".

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	
(S) The	Slide#5
(S) The	
(S) Slide photo is mailbox near Ames' residence Slide photo is park sign near Hanssen's residence On these slides, the instructor should emphasize	Slides#6,7,8 Photos of and sites

b1
b7E

b1
b7E

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
	Slide#9
(S)	
(S)	Slides#10,11,12 Photos of actual
	Slide #13
(S)	
(S)	
(S)	Slide #14
(S)	
	Slide #15
(S)	
(S)	

b1
b7E

b1
b7E

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	Slide #16
(S)	
	Slide #17
(S)	
(S)	

b1
b7E

Outline of Activities

Content Outline/Activities	Instructor Notes
(S)	Slide #18
(S)	
	Slide #19 "Packages"
(S)	
	Slide #20 "Other Clandestine Communications."
(S)	

b1
b7E

b1
b7E

b1
b7E

Outline of Activities

(S)

Content Outline/Activities	Instructor Notes
(S) (S) (S)	Slide #21 "Tools of the Trade"
"Internet"	Slide #22 "Clandestine Communications-The Next Generation"
(S) (S)	
"Electronic Devices"	
(S) (S) (S)	
(S)	Slide #23 "Clandestine Communications-The Next Generation?"

b1
b7E

b1
b7E

b1
b7E

b1
b7E

Outline of Activities

(S) Content Outline/Activities	Instructor Notes
(S)	b1 b7E
	Slide #24 "Clandestine Communications-The Next Generation?"
(S) "The Internet"	
(S)	b1 b7E
	Slide # 25 "Training"
"Training"	b1 b7E
(S)	
	Slide #26 " Trends"
(S) "UNIVERSAL" - The methods and techniques of the services are very similar, although some differences will be exhibited	b1 b7E

ACLURM032149

Outline of Activities

(S)

Content Outline/Activities	Instructor Notes
(S) Slides #27-36 [redacted]	Slides #27-36 [redacted]
[redacted]	
Instructor Points:	
(S) [redacted]	
Summary At this time, the instructor may field questions from the class, bearing in mind that subsequent blocks of instruction will provide more in-depth information regarding many of the principle discussed in this introductory class.	

b1
b7E

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Statement of Objectives

Instructional Goal:

(S) After the block of instruction, the student will posses an awareness, and have the ability to recognize various forms of [redacted]

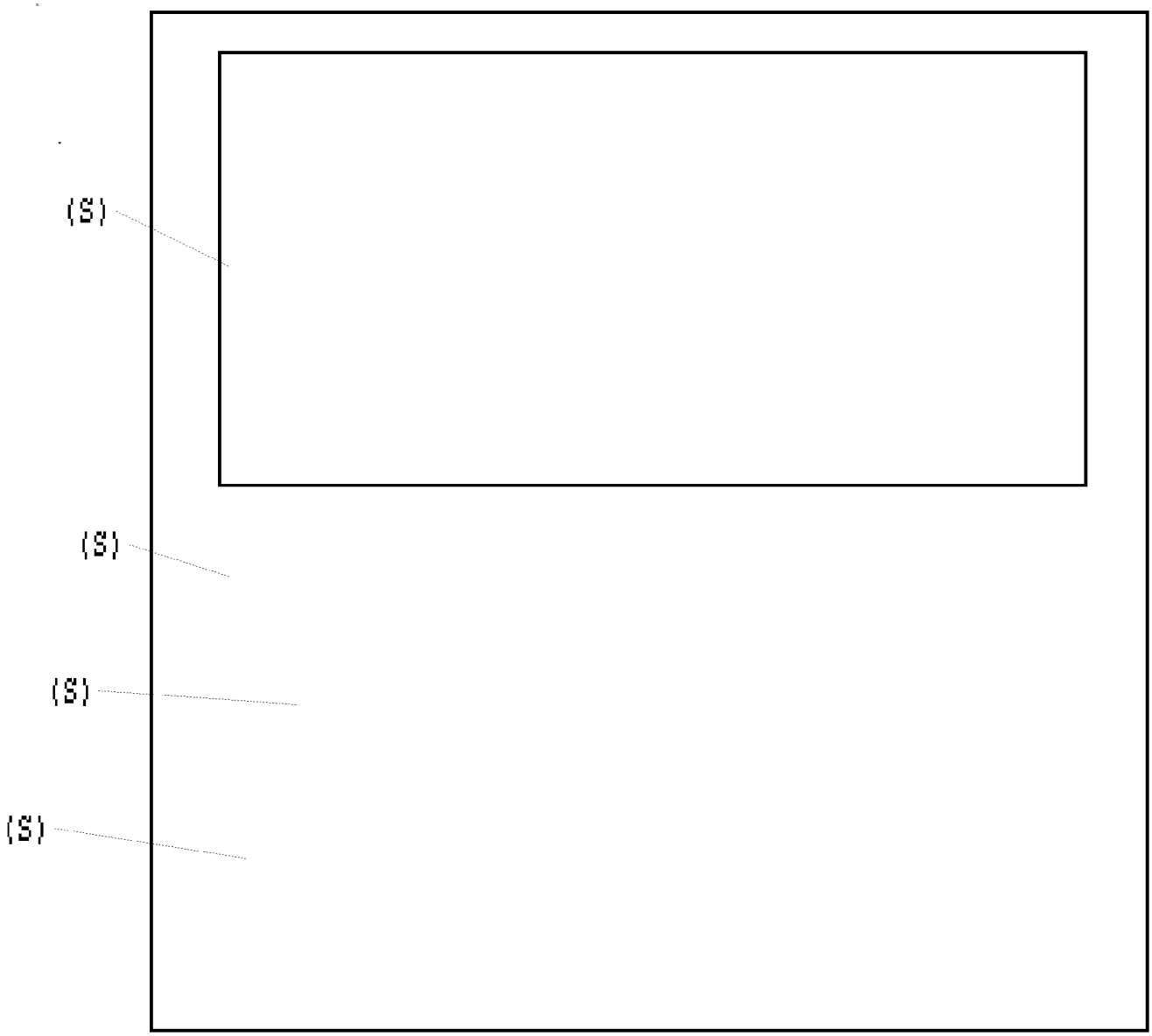
b1
b7E

Instructional Objective:

After two hours of instruction, students will, from memory:

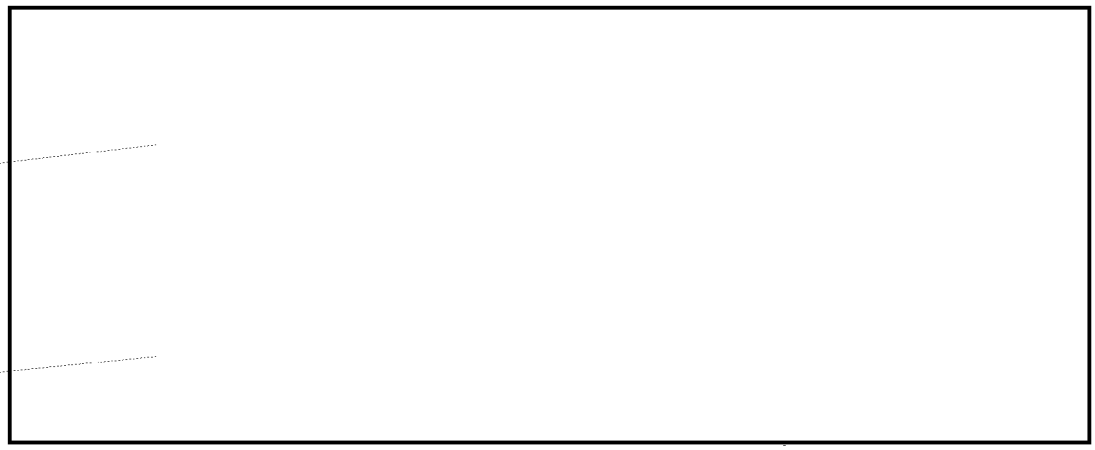
1. Be able to name the three types of operational acts.
2. Have the ability to identify no less than 5 operational acts by definition.

Test



b1
b7E

Test Answers



(S)

(S)

b1
b7E

ACLURM032153
FBI031673

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-10-2037

22 **Teaching Point**

To acquaint the student with the [redacted]

Comment

See slide for comments

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b7E

[redacted]

23 **Teaching Point**

To acquaint the student with [redacted]

Comment

[redacted]

b7E

24 **Teaching Point**

[redacted]

Comment

Definition of: [redacted]

b7E

[redacted]

b7E

[redacted]

The word "rootkit" came to public awareness in the 2005 Sony CD copy protection scandal, in which Sony BMG music CDs surreptitiously placed a rootkit on Microsoft Windows PCs when the CD was played on the computer. Sony provided no mention of this in the CD or its packaging, referring only to security rights management measures.

25 **Comment**

[redacted]

b7E

The word "rootkit" came to public awareness in the 2005 Sony CD copy protection controversy, in which Sony BMG music CDs placed a rootkit on Microsoft Windows PCs.

26 **Teaching Point**

To acquaint the student with steganography which can be used to conceal information.

Comment

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured.[1]

Steganography simply takes one piece of information and hides it within another. Computer files (images, sounds recordings, even disks) contain unused or insignificant areas of data. Steganography takes advantage of these areas, replacing them with information (encrypted mail, for instance). The files can then be exchanged without anyone knowing what really lies inside of them. An image of the space shuttle landing might contain a private letter to a friend. A recording of a short sentence might contain your company's plans for a secret new product. Steganography can also be used to place a hidden "trademark" in images, music, and software, a technique referred to as watermarking.

b7E

[1] http://en.wikipedia.org/wiki/Steganography

27 **Comment**

[redacted]

b7E

[redacted]

b7E

28 **Teaching Point**

To acquaint the student with use of Satellites for Audio Interception and Photography.

Comment

A spy satellite (officially referred to as a reconnaissance satellite or recon sat) is an Earth observation satellite or communications satellite deployed for military or intelligence applications. Until the 1970s and even the 1980s, many reconnaissance satellites that took photographs would eject canisters of photographic film, which would descend to earth and be retrieved in mid-air as they floated down on parachutes.[1]

The first satellites ejected canisters.

1 http://en.wikipedia.org/wiki/Reconnaissance_satellite

29 **Training Point**

Provide the student an understanding of the basic facts of the espionage case pertaining to Andrew Daulton Lee and Christopher Boyce who compromised US satellite systems.

Comment

Andrew Daulton Lee and Christopher Boyce. United States citizens and Los Angeles natives, were portrayed by actor Sean Penn in director John Schlesinger's 1985 movie *The Falcon and the Snowman* based on the book by Robert Lindsey. The book and the film documented the true to life espionage activities of Lee (a heroin and cocaine dealer by trade, hence his nickname, "The Snowman") and his childhood friend Christopher Boyce during the mid-1970s. The Boyce character (nicknamed "The Falcon" because of his long interest in the sport of falconry) was played in the film by actor Timothy Hutton.

For nearly two years, Lee (the adopted eldest son of a wealthy physician) traveled to Mexico City operating as the courier for an espionage scheme which had consisted of his delivering to Soviet Embassy officials classified documents concerning how to decrypt secure US government message traffic and detailed specifications of the latest US spy satellites. These documents were supplied by Boyce, a code clerk employed with the large US defense contractor TRW, headquartered in the Los Angeles community of Redondo Beach. Boyce (whose father was an aerospace

corporation security officer and a retired FBI agent) held a top secret clearance and worked in the company's "Black Vault" (classified communications center.)[1]

[1] http://en.wikipedia.org/wiki/Andrew_Daulton_Lee

30 **Teaching Point**

To provide an understanding of the wide use of satellite photography to collect intelligence.

Comment

[redacted] b7E

31 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of effective devices that can be used to collect and communicate intelligence information.

Comment

See slide for description of device.1

1 www.asisonline.org/lac/executive/teletech.ppt

32 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

New Audio Recorders with USB connectivity.

See slide for description of device.[1]

1 www.asisonline.org/lac/executive/teletech.ppt

33 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

[redacted] b7E

[redacted]

b7E

34 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

[redacted]

b7E

The following is from the skype.com FACs:

Is Skype secure?

Yes. When you call another Skype user your call is encrypted with strong encryption algorithms ensuring you privacy. In some cases your Skype communication may be routed via other users in the peer-to-peer network. Skype encryption protects you from potential eavesdropping from malicious users.

35 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

[redacted]

b7E

b7E

[redacted]

b7E

36 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Casio Audio Recorder:

30 Second Record capability

30 Pages of TeleMemo Data

$69

MP3 watches also available

37 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Micro Camera

- 300 Foot Transmission Range
- Operates on a Single 9 Volt Battery
- Matching Wireless Receiver Included
- Field Of View 60 Degrees
- Pinhole Style Lens
- $79 - $99 with audio capability

38 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Scanner Pen

- Handheld Scanner
- Top model can store
- 3000 pages of text
- Has IR transfer capability
- $100 - $200

39 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Casio Watch Camera:

- Recording system JPEG (176 x 144 pixels), 16,770,000- color data
- Recording medium Built-in Flash Memory (1 MB)
- Memory capacity Up to 100 images*1 (JPEG format); auto memory of shooting date/time
- Focusing distance approx. 30 cm, compensation possible Zoom 2X digital zoom
- Shooting mode Outdoor, Indoor, Dusk; brightness control
- Databank function Up to 24 characters/image (uppercase alphabetic characters, numbers, symbols), thumbnail search function
- IR Data Communication, range 10 cm max

40 **Teaching Points**

To acquaint the student with the affect of new technology on the availability of various effective devices that can be used to collect and communicate intelligence information.

Comment

Pen Cam Mega P-3

- Multi-function : Digital still camera/PC camera/digital camcorder
    - megapixel CMOSInternal memory
- Image capacity - 8 MB built-in SDRAM (for avi movies)116 MB built-in Flash memory (for digital stills)

- 1248 x 960- up to 50 pictures
- 640 x 480- up to 160 pictures AVI
- Dimensions - 1.61 x 1.34 x 4.6 inches;
- 68 grams (without battery)

41 **Teaching Point**

Agents can innovate and create their own techniques to communicate sensitive intelligence. b7E per FBI

Comment

[redacted]

42 **Teaching Point**

There are various methods by which we can counter the cyber threat.

Comment

See slide and describe each of the capabilities listed. b1 per FBI b7E

Note a weakness is that we can have procedures and rules and fail to follow them. For example,

(S) [redacted]

b7E per FBI

[redacted]

43 **Comment**

Will cover in this segment a few comments about the following techniques:

Referral/Direct

(S) [redacted]

- Recruitments
- National Clandestine Service (NCS)

b1 per FBI
b7E

(S) 44 **Comment**

[redacted]

Pitts

Lessenthien

Trofimov

45 **Comment**

(S) [redacted] Earl Pitts.

46 **Comment**

(S) [redacted] Kurt Lessenthein.

b1 per FBI
b7E

47 **Comment**

(S) [redacted] George Trofimoff.

48 **Comment**

(S) Recruitment

Discuss the benefits of recruitment i.e. Hanssen [redacted]

49 **Comment**

National Clandestine Service (NCS)

The new entity will oversee human intelligence operations conducted by the 15 U.S. agencies involved in spying, including the FBI and the Defense Intelligence Agency, a branch of the Pentagon. "This is another positive step in building an intelligence community that is more unified, coordinated and effective, and is better positioned to meet the increasingly complex intelligence challenges of the future," said John D. Negroponte, director of national intelligence. "The NCS will serve as the national authority for the integration, coordination, de-confliction and evaluation of human intelligence operations across the entire intelligence

community," Negroponte said in a news release.

b1
b7E

(S) **Goal**: To instill in the student an understanding of the significant issues and techniques relating to [redacted]

(S) **Objective**: To provide the student with a comprehensive and lively explanation of the use of contemporary [redacted]

Criterion Test Questions:

b1
b7E

(S) [redacted]

b1
b7E

18. What is [redacted]

(S) 19. Name two cases where the [redacted] technique was used.

20. What is the name of the new entity that will oversee human intelligence operations conducted by 15 U.S. agencies?

Test Answers:

(S)

(S)

b1
b7E

b7E

[redacted]

Equipment:

Equipment/Aids for Instructor: Power Point Projector and VHS

Equipment/Aids Required for Instructor: Power Point projector and VCR

Equipment/Aids Required for Students: None.

Power Point Slides or Overheads: Power Point Slides.

Handouts: Yes.

Bibliography:

Ronald Kessler. *Moscow Station*. New York: Charles Scribner's Sons, 1989.

Ronald Kessler. *The Spy in the Russian Club*: Charles Scribner's Sons, 1990.

Sherry Sontag and Christopher Drew. *Blind Man's Bluff*. New York: Public Affairs, 1998.

David Wise. *Spy*. New York: Random House, 2002.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 01-10-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c,d)
DECLASSIFY ON: 01-10-2037

Course 2A – *Early* [redacted]
June 6, 2006

Federal Bureau of Investigation

Title of Instruction: [redacted]

b6
b7C
b7E

Time of Instruction: Two (2) Hours.

Target Group: FBI Special Agents and other selected personnel.

Instructor: [redacted]

Method of Instruction: Lecture, group discussion

Additional Information: None

February 1, 2008.

(S) **Goal**: To instill in the student an understanding of the significant issues and techniques relating to [redacted]

b1
b7E

Objective: To provide the student with a comprehensive and lively explanation of the use of [redacted]

(S)

Lesson Plan

[redacted]

Slide #	*Teaching Points/Comments*
1	Introduction
2	**Teaching Point:** Provide a definition of [redacted] and explain where it fits in understanding an intelligence operation.

b1
b7E

Comment:

(S) [redacted]

3 **Teaching Point:**

(S) [redacted]

[redacted]

b1
b7E

Comment:

(S) [redacted]

4 **Teaching Point:**

(S) [redacted]

b1
b7E

Comment:

(S) [redacted]

5 **Teaching Point:**

Communication can be made in secret writing.

Comment:

Explain the difference between cryptology and cryptography.

6 **Teaching Point:**

[redacted]

b7E

Comment:

[redacted]

7 **Teaching Point:**

[redacted]

8 **Teaching Point:**

[redacted]

b7E

decrypt the message.

Comment:

[redacted]

9 **Comment:**

Second click produces the translation - Point out the key words in it to illustrate the method of communication.

10 **Teaching Point**:

(S) [redacted]

b1
b7E

(Photos of secret writing containers and examples of secret writing used during the American Revolutionary War).

11 **Comment:**

[redacted]

b7E

12 **Teaching Point:**

Many apparently innocent items can be used to hide secret messages. b7E

Comment:

[redacted]

13 **Teaching Point:**

[redacted]

Comment:

[redacted] b7E

14 **Teaching Point:**

Some relatively simple methods can be highly effective.

Comment:

(S) [redacted] b1 b7E

15 **Teaching Point:**

[redacted]

Comment:

[redacted] b7E

16 **Teaching Point:**

[redacted]

b7E

Comments

[redacted]

b7E

17,18,19,20, **Teaching Point:**

Acquaint the student with [redacted]

Comment:

[redacted]

b7E

21 **Teaching Point**

[redacted]

Comment

b7E

[redacted]

22, 23 **Teaching Point:**

Acquaint the student with the use of [redacted]

Comment:

b7E

[redacted]

b7E

[redacted]

24 **Teaching Point:**

To acquaint the student with [redacted]

[redacted]

Comment:

b7E

[redacted]

25 **Teaching Point:**

To acquaint the student with [redacted]

[redacted]

Comment:

b7E

[redacted]

26 **Teaching Point:**

To acquaint the student with the concept of [redacted]

Comment:

[redacted]

27 **Teaching Point:**

To acquaint the student with the concept of [redacted]

Comment:

(Examples of Ames and Hanssen) b7E

28 **Teaching Point:**

To acquaint the student with the [redacted]

Comment:

(Lonetree and Hanin Cases)

29 **Teaching Point:**

(S) [redacted] b1 b7E

Comment:

[redacted]

30 **Introduction to Segment re Clandestine Electronic Devices**

31 **Teaching Point:**

To acquaint the student with the various different kinds of electronic devices utilized in espionage transactions.

Comment

Describe devices listed in slide.

- Listening Devices

(S) [redacted] b1 b7E

b7E

32 **Teaching Point**

Listening devices can be placed surreptitiously to collect information.

Comment

(S) [redacted]

33 **Teaching Point**

(S) [redacted]

b1
b7E

Comment

(S) [redacted]

34 **Introduction to Segment re Spy Cameras**

35 **Comment**

[redacted]

b7E

36 **Segment re Concealed Devices**

37 **Teaching Point**

A variety of common devices found in many homes or offices have been used to secrete intelligence.

Comment

A variety of common, everyday devices have been utilized by intelligence services to enable their agents to conceal information and equipment. Several of these devices appear on this and the following slides.

38 **Teaching Point**

The situation drives the design of the concealment.

39 **Comment**

[redacted]

40 **Comment**

Everyone has one or more of these.

41 **Introduce Segment re** [redacted] **is Countered**

42 **Teaching Point**

(S) [redacted]

Comment

The methods that will be discussed are listed on the slide.

b1
b7E

43 **Teaching Point**

(S) [redacted]

Comment

(S) [redacted]

44 **Teaching Point**

(S) [redacted]

Comment

b1
b7E

(S) [redacted]

Mention also:

[redacted]

45 **Teaching Point**

[redacted]

Comment

b7E

[redacted]

b7E

46 **Teaching Point**

[redacted]

Comment

Describe the Verona Case and what it revealed about Soviet intelligence operations and activities in the US. Julius and Ethel Rosenberg were guilty.

Point out how difficult it is today to break encrypted messages.

47 **Teaching Point**

Video may be used to surveil an espionage meeting, [redacted] b7E
or a variety of other intelligence activities.

Comment

Generally, video is an important technique when CI has an idea of where an activity may occur. Then the placement of video cameras may collect intelligence or evidence to be used in a prosecution.

48 **Comment**

[redacted]

49 **Teaching Point**

(S) To acquaint the student with the technique of surveillance [redacted]

[redacted]

Comment b1 b7E

(S) [redacted]

50 **Teaching Point:**

To acquaint the students with the reasons for conducting surveillances.

Comment

There are various reasons for conducting surveillances, not just to observe the subject. [redacted] b7E

b7E

[redacted]

51 **Teaching Point:**

To acquaint the student with the different types of surveillance

Comment

[redacted]

b7E

52 **Teaching Point**

To acquaint the student with the technique of [redacted]

Comment

[redacted]

b7E

53 **Training Point**

[redacted]

(S)

Comment

DISCUSS THE BENEFITS OF RECRUITMENT citing cases involving Oleg Gordievsky, Boris Yuzhin, Kim Philby, and Vasili Mitrokhin. Discuss the impact of the Robert Hanssen case on the FBI and of the Aldrich Ames case on the CIA.

b1
b7E

(S)

[redacted]

Photos are of Arkady Shevchecnko, Mitrokin, Philby, Guy Burgess, Donald Maclean, Ed Howard, Ames, Hanssen, Felix Block, Dmitri F. Polyakov, Valeri Martynov, and Sergei Motorin .

Criterion Test Questions:

(S) [redacted]

b1
b7E

Test Answers:

[redacted]

b7E

(S) [redacted]

b1
b7E

(S) [redacted]

(S) [redacted]

Equipment:

Equipment/Aids for Instructor: Power Point Projector and VHS

Equipment/Aids Required for Instructor: Power Point projector and VCR

Equipment/Aids Required for Students: None.

Power Point Slides or Overheads: Power Point Slides.

Handouts: Yes.

Bibliography:

Ronald Kessler. *Moscow Station*. New York: Charles Scribner's Sons, 1989.

Ronald Kessler. *The Spy in the Russian Club*: Charles Scribner's Sons, 1990.

Sherry Sontag and Christopher Drew. *Blind Man's Bluff*. New York: Public Affairs, 1998.

David Wise. *Spy*. New York: Random House, 2002.

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

CONTEMPORARY [redacted]

Contemporar[redacted]

Agenda

1. Contemporary [redacted] Defined
2. Old Spies and New Focus
3. Old Problems and New Techniques
4. Cyber Attacks
5. Stenanography
6. Satellite Interception
7. Gizmos

Contemporary [redacted]

b7E

Contemporary [redacted] Defined

[redacted]

Contemporary [redacted]

Old Spies and New Focus

Information vs. Bullets



Image:cnn.com

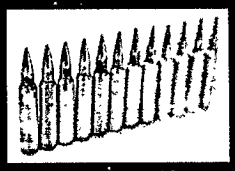


Image:flickr.com

Contempor[redacted]

b7E

Old Spies and New Focus

Friend or Foe

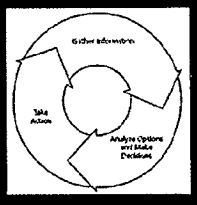


Image:Amazon.com

Contemporar[redacted]

Old Spies and New Focus

Information Gathering



Contempor[redacted]

b7E

~~SECRET~~

ACLURM032180

FBI031700

Old Spies and New Focus

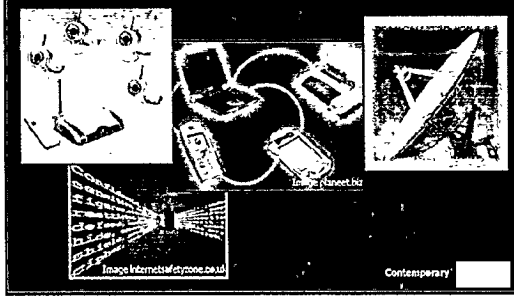
Diminished Personal Risk



Contemporary

Old Problems and New Techniques

Communicating

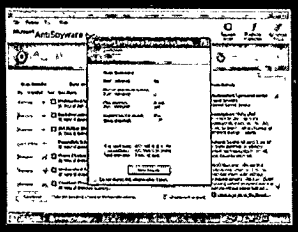


Contemporary

b7E

Old Problems and New Techniques

Malware Utilization



Contemporary

Cyber Attacks

- Malware
  - Virus
  - Worms
  - Trojan Horse
- Spoofing
- Phishing
- Spector and Spector CNE
- eBlaster
- Rootkit

Contempora

b7E

Cyber Attacks



Virus

A virus is a self-replicating/self-reproducing-automation program that spreads by inserting copies of itself into other executable code or documents.

A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells.

Extending the analogy, the insertion of a virus into the program is termed as an "infection".

Contemporar

Cyber Attacks

Virus

The infected file (or executable code that is not part of a file) is called a "host". Viruses generally do not affect network performance, as their malicious activities are mostly confined within the target computer itself.

Viruses are one of the several types of malicious software or malware

Predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

Contempora

b7E

ACLURM032181



Cyber Attacks

Virus

~~Some viruses have a delayed payload, which is sometimes~~ called a bomb.

For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts.

A time bomb occurs during a particular date or time.

A logic bomb occurs when the user of a computer takes an action that triggers the bomb.

Contemporar

Cyber Attacks

Worms



A computer worm is a self-replicating computer program, similar to a computer virus.

A worm is self-contained and does not need to be part of another program to propagate itself.

Contempori

b7E

Cyber Attacks

Worms

They are often designed to exploit the file transmission capabilities found on many computers.

The main difference between a computer virus and a worm is that a virus cannot propagate by itself whereas worms can.

A worm uses a network to send copies of itself to other systems and it does so without any intervention.

In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer.

Contemporar 5

Cyber Attacks

Trojan Horse



- **A Trojan horse** is a malicious program that is disguised as legitimate software.
- The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed.

Contemporan 6

b7E

Cyber Attacks

Trojan Horse

Two common types of Trojan horses:

1. Corrupting useful software, a cracker inserts malicious code that executes while the program is used.
2. Masquerading standalone program as something else
   1.

Contemporary 7

Cyber Attacks

Spoofing

- A technique used to gain unauthorized access to computers.
- The intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Contemporary 8

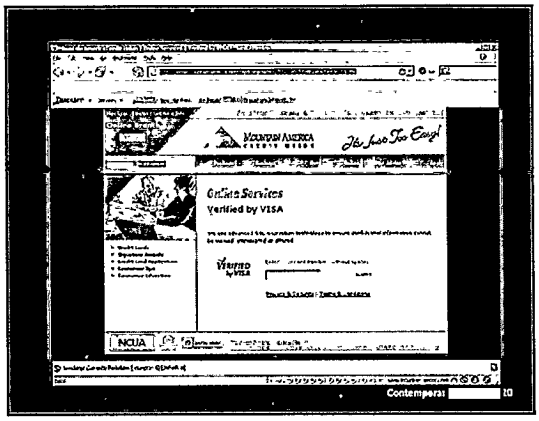
b7E

Phishing

Cyber Attacks

- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
- The e-mail directs the user to visit a bogus Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has.
- The Web site is set up only to steal the user's information.

Contemporary 9



Contemporar 10

b7E

Cyber Attacks



Spector and Spector CNE

- The Most Intelligent Internet Monitoring and Surveillance Software available. Rated #1 spy software by PC Magazine.
- Records Emails, Chats, IMs, Web Sites, Programs Run, Keystrokes Typed, Peer to Peer File Sharing, Screen Snapshots –

  Plus - Offers Internet Access Blocking and Instant Notification Alerts.

Contemporar 11

Spector and Spector CNE

Cyber Attacks

Spector CNE:

Corporate se: automatically captures and lets you review your employees'

- emails sent and received
- chat conversations and instant messages
- files downloaded
- web sites visited
- applications launched
- keystrokes typed

Spector CNE is the Corporate Network Edition of Spector Pro - winner of the PC Magazine Editors' Choice Award for Best Activity Monitoring Software

Contempora 12

b7E

Cyber Attacks

eBlaster

- The ONLY software in the world that will capture their incoming and outgoing email, chats and instant messages - then IMMEDIATELY forward you an EXACT COPY



Contempora 13

Cyber Attacks

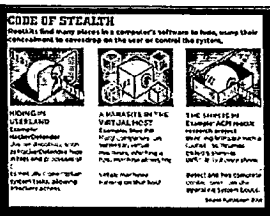
Rootkit

- Rootkit: a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system.
- These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's knowledge.

Contemporan 14

b7E

Rootkit



Cyber Attacks

- Rootkits are known to exist for a variety of operating systems such as Linux, Solaris and versions of Microsoft Windows.
- A computer with a rootkit on it is called a rooted computer.
- The word "rootkit" came to public awareness in the 2005 Sony CD copy protection controversy, in which Sony BMG music CDs placed a rootkit on Microsoft Windows PCs

Contemporary [redacted] 25

Steganography

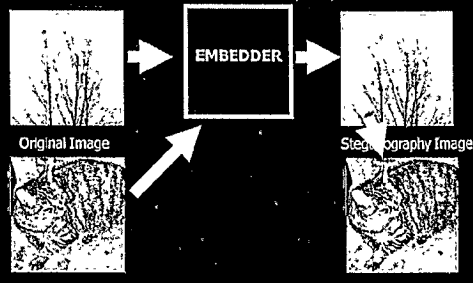


Image wikipedia.org

Contemporar [redacted] 15

b7E

Steganography



Images wikipedia.org

Contempora [redacted] 7

Satellite Audio Interception and Photography

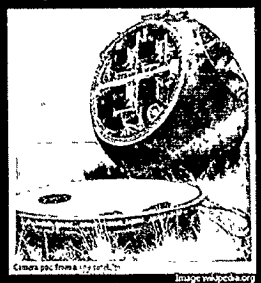


Image wikipedia.org

Contemporar [redacted] 5

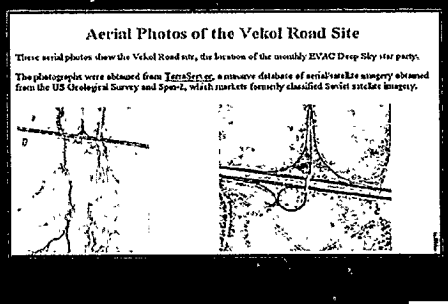
b7E

Satellite Audio Interception and Photography



Contemporary [redacted] 9

Satellite Audio Interception and Photography



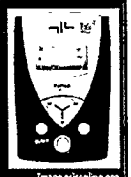
Contemporary [redacted] 0

b7E

Audio Gizmos

RipFlashtm Plus Features:

MP3/WMA (Windows tm Media Audio) Player and MP3 Recorder 128MB Four Hour CD Quality (WMA) Playback (2hourMP3 Record) Up to 30 Hour Voice Recording (MP3 encoded)



Backlit Display with full ID3 tag data

Compact size ; 2.32 x 3.46 x0.67 in (WxHxD)

Built -in Microphone and Speaker (MP3 Voice Recording)

Line-in for direct recording from any analog audio source

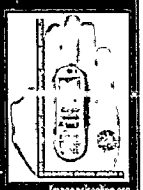
Smart Media Card Memory Expansion Slot

Contemporary 1

Audio Gizmos

Olympus DS-660 Features:

32MB of built-in memory; up to 11 hours recording time.



USB docking station

Voice Activation -- automatically begins and stops recording as it senses volume

Recording time: SP mode - 5 H; LP mode –11 H

Site – 108 x 41.5 x 21 mm

Weight – 75g (including batteries)

Contemporz

b7E

Audio Gizmos

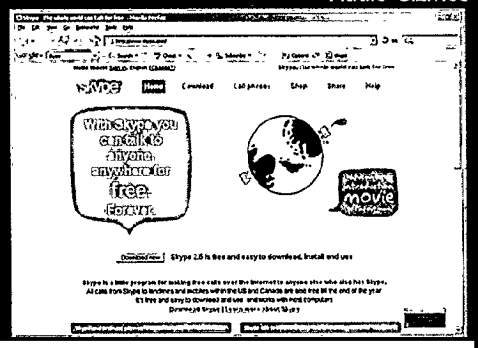
Spy Phone (Unlocked) » $1,799.00
Standard
Triband GSM: 1900 / 900 / 1800 (Works Worldwide)
Weight 76g, **Dimensions**102mm x 44mm x 13mm
Display Monochrome,
Battery Talk Time: 300 mins, Standby: 260 hrs
Features



- Built in Speakerphone
- You can listen in on whoever takes the spy phone at anytime.
- Can dial out and receive any phone call, like any other cell phone.
- Transmission occurs only when the eavesdropper calls the cellular bug from a preprogrammed number.

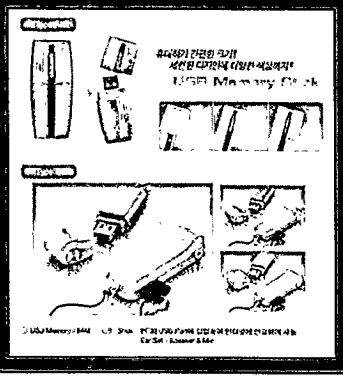
Contemporan 3

Audio Gizmos



b7E

Audio Gizmos



Contemporan 5

Audio Gizmos

Casio Audio Recorder:

30 Second Record capability

30 Pages of TeleMemo Data

$69

MP3 watches also available



Contemporar 5

b7E

ACLURM032185

Video/Photo Gizmos

Micro Camera

- 300 Foot Transmission Range
- Operates on a Single 9 Volt Battery
- Matching Wireless Receiver Included
- Field Of View 60 Degrees
- Pinhole Style Lens
- $79 - $99 with audio capability

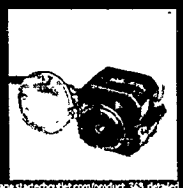


Image startechoutlet.com/product_343_detailed

Contempora

Video/Photo Gizmos

Scanner Pen

- Handheld Scanner
- Top model can store
- 3000 pages of text
- Has IR transfer capability
- $100 - $200



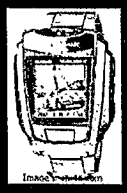
Image cnet.com/sc

Contemporar

b7E

Video/Photo Gizmos

Casio Watch Camera:



- ■Recording system JPEG (176 x 144 pixels), 16,770,000- color data
- ■Recording medium Built-in Flash Memory (1 MB)
- ■Memory capacity Up to 100 images*1 (JPEG format); auto memory of shooting date/time
- Focusing distance approx. 30 cm, compensation possible Zoom 2X digital zoom
- Shooting mode Outdoor, Indoor, Dusk; brightness control
- Databank function Up to 24 characters/image (uppercase alphabetic characters, numbers, symbols), thumbnail search function
- IR Data Communication, range 10 cm max

Contemporar 9

Video/Photo Gizmos

Pen Cam Mega P-3

Multi-function : Digital still camera/PC camera/digital camcorder

1.3 megapixel CMOSInternal memory

Image capacity - 8 MB built-in SDRAM (for avi movies)116 MB built-in Flash memory (for digital stills)

1248 x 960- up to 50 pictures

640 x 480- up to 160 pictures AVI

Dimensions - 1.61 x 1.34 x 4.6 inches;

68 grams (without battery)

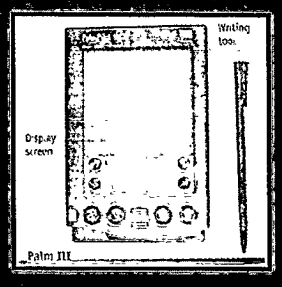


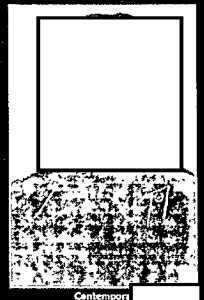
Image shopsite.rnil.com/media/DRproducts

Contemporar 10

b7E

Gizmos





Contempora

Countering the Cyber Threat

Contemporan

b7E

(S)

(S)

Countering the Human Threat

[redacted]

- Recruitments
- National Clandestine Service (NCS)

Contemporary [redacted]

Countering the Human Threat

[redacted]

Pitts

Lessenthien

Trofimov

Contemporary [redacted]

b1
b7E

(S)

(S) [redacted]

Earl Pitts



Pitts (CNN/file)

Contemporary [redacted]

[redacted]

Kurt Lessenthein



Conte [redacted]

b1
b7E

(S) [redacted]

George Trofimoff



Contemporary [redacted]

Countering the Human Threat

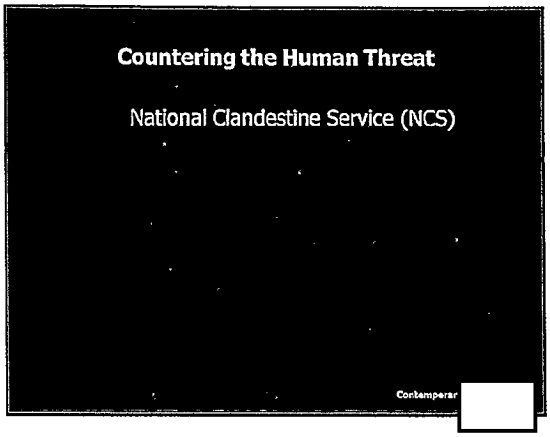
Recruitments

Contemp [redacted]

b1
b7E

ACLURM032187

FBI031707

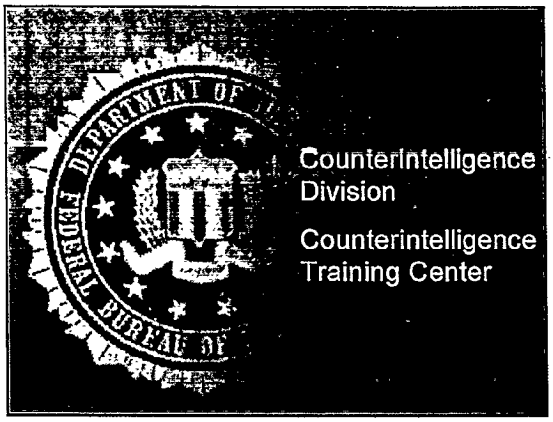

Countering the Human Threat
National Clandestine Service (NCS)
Contemporar

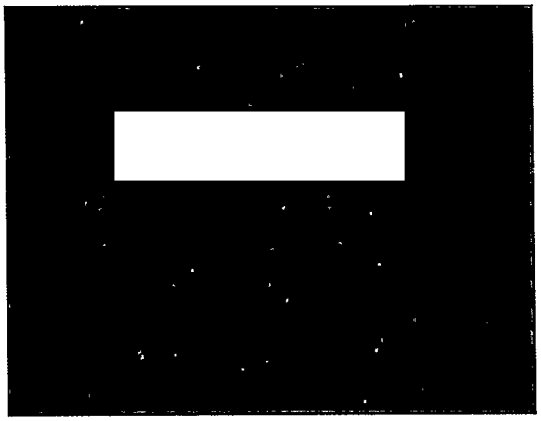
b7E

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

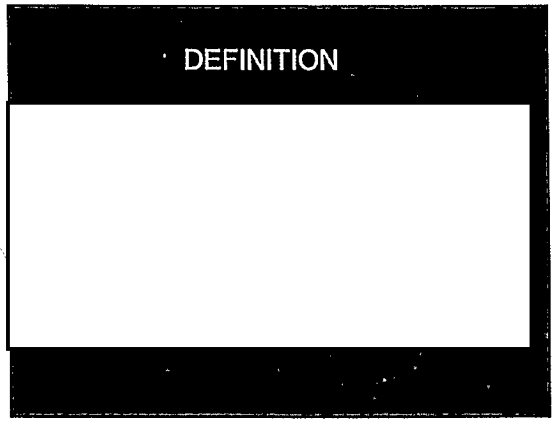
7/15/2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

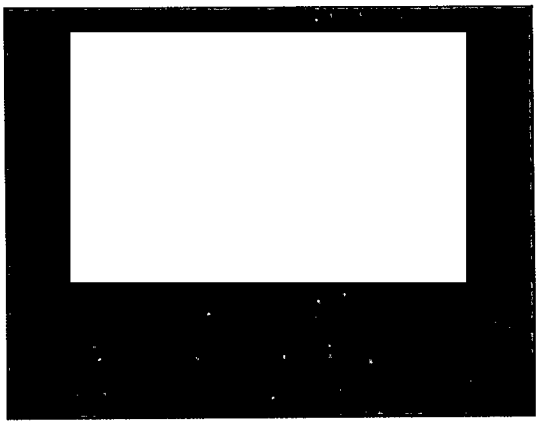




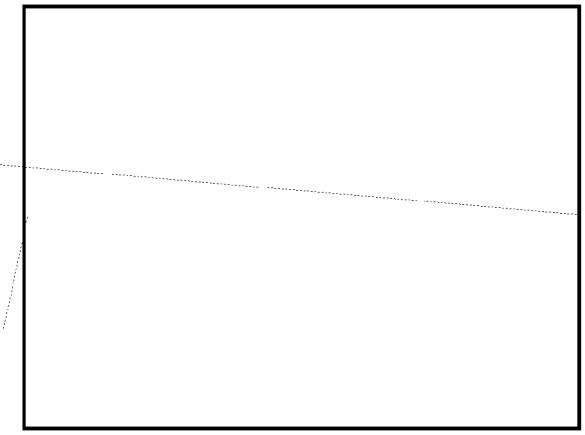
b7E



(S)

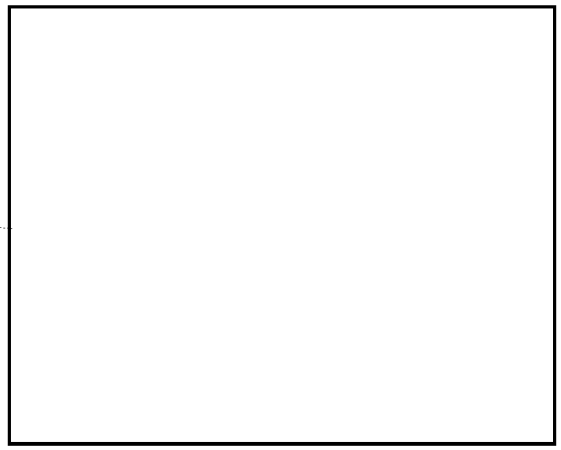


b1
b7E



(S)

(S)



b1
b7E

ACLURM032189

(S)

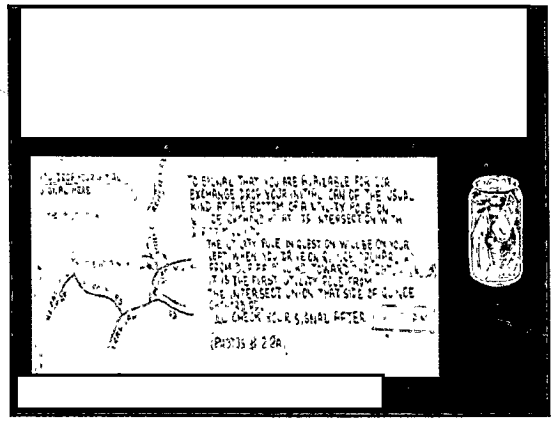
- TOOLS

(S)

(S)

b1
b7E

(S)





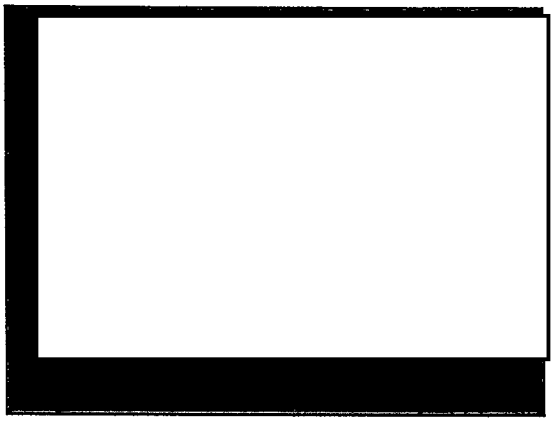
b1
b7E

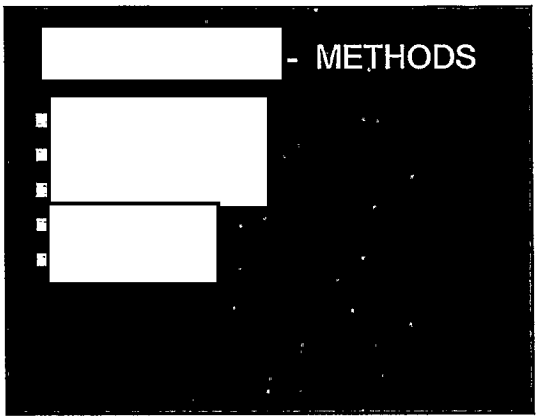
(S)

- Communications

(S)

b1
b7E

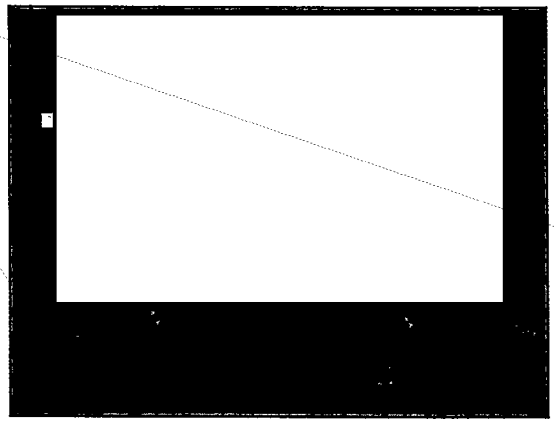


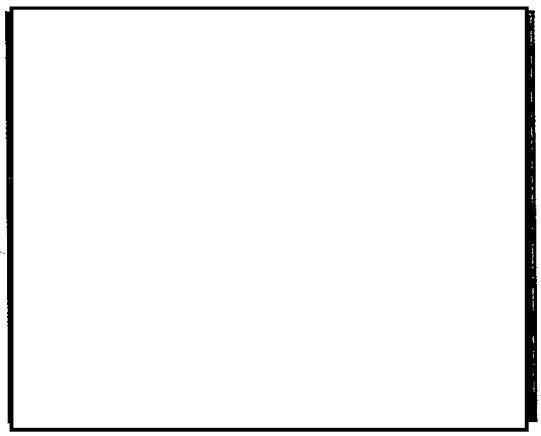


b7E

(S)

(S)

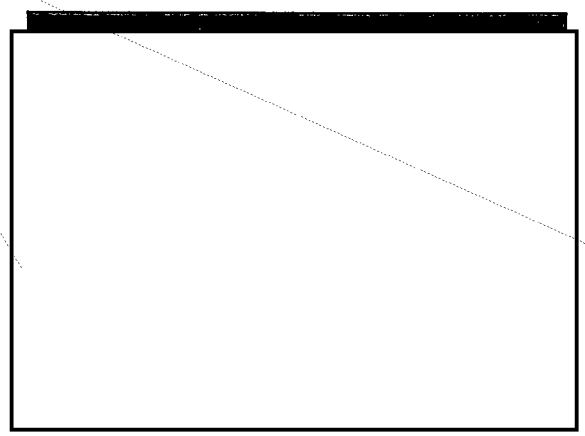


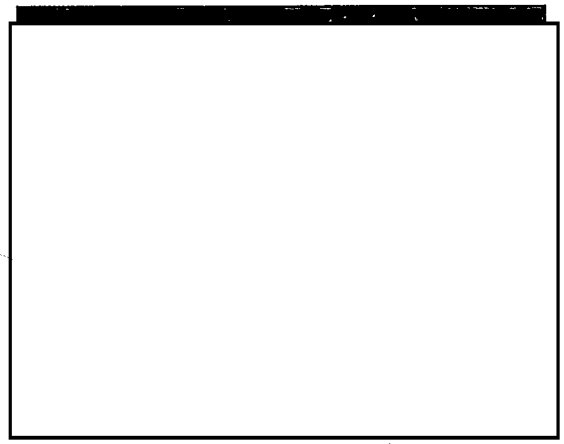


b1
b7E

(S)

(S)





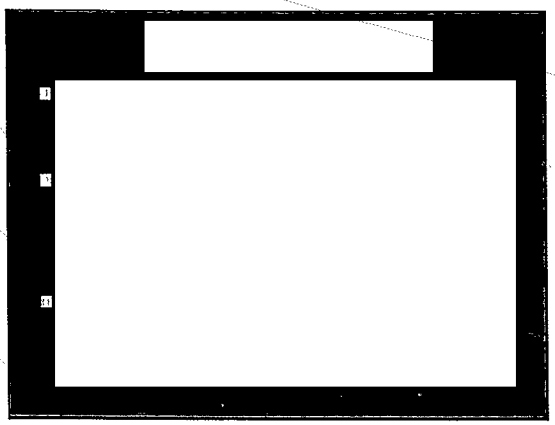
b1
b7E

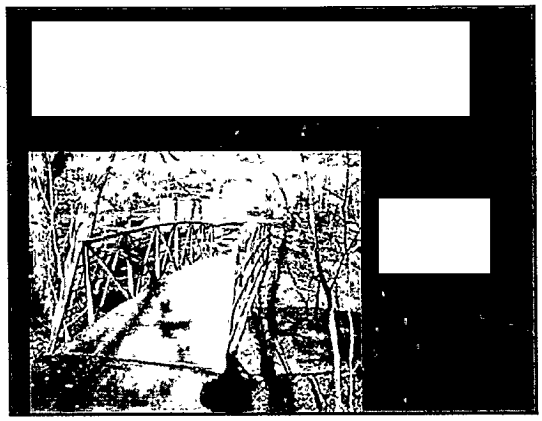
(S)

(S)

(S)

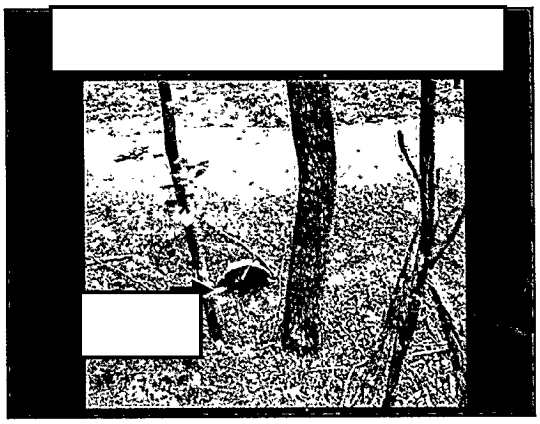
(S)





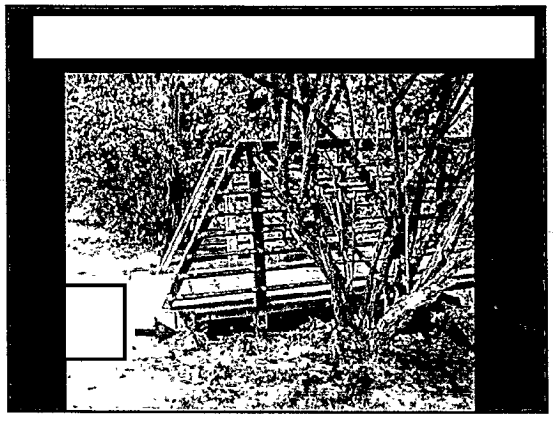
b1
b7E

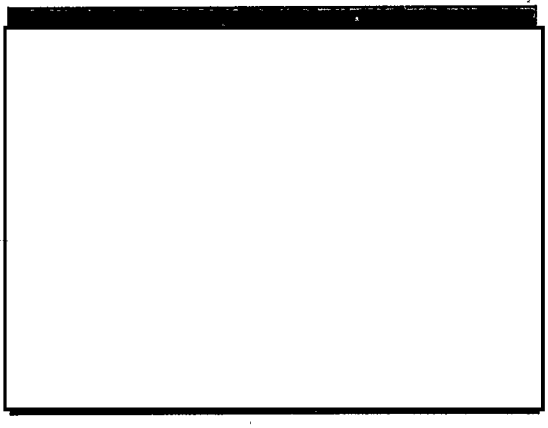




b7E

(S)





b1
b7E

(S)

(S)

b1
b7E

(S)

EQUIPMENT

- Concealment Devices
- Photography
  - Cameras
  - Scanners

Concealment Devices

b1
b7E

Document Photography

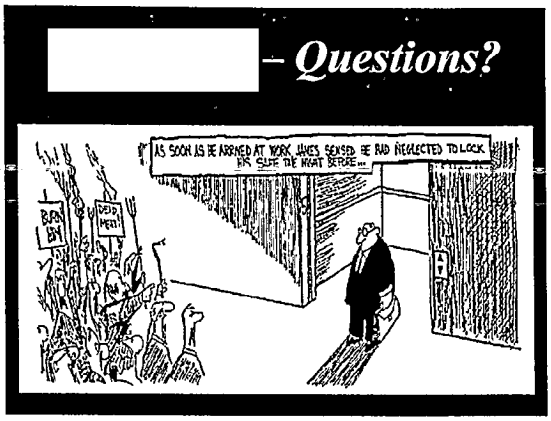


Concealment Devices

b7E

ACLURM032194

FBI031714


– Questions?
AS SOON AS HE ARRIVED AT WORK JAMES SENSED HE HAD NEGLECTED TO LOCK HIS SUITE THE NIGHT BEFORE...

b7E

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/EAW/STP/bls
REASON: 1.4 (c,d)
DECLASSIFY ON: 01-11-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Federal Bureau of Investigation

Title of Instruction: [redacted]

Time of Instruction: Two (2) Hours.

Target Group: FBI Special Agents and other selected personnel.

Instructor: [redacted]

Method of Instruction: Lecture, group discussion

Additional Information: None

February 1, 2008.

b6
b7C
b7E

(S) **Goal**: To instill in the student an understanding of the significant issues and techniques relating to [redacted]

(S) **Objective**: To provide the student with a comprehensive and lively explanation of the use of [redacted]

b1
b7E

Lesson Plan

[redacted]

b7E

Slide #	*Teaching Points/Comments*
1	Introduction
2	**Teaching Point:** Provide a definition of [redacted] and explain where it fits in understanding an intelligence operation.

ACLURM032196
FBI031716

		Comment:
	3	**Teaching Point:**
		Comment:
	4	**Teaching Point:**
		Comment:
	5	**Teaching Point:** Communication can be made in secret writing. **Comment:** Explain the difference between cryptology and cryptography.
	6	**Teaching Point:**
		Comment:

(S)

(S)

(S)

(S)

(S)

(S)

b1
b7E

b1
b7E

b1
b7E

7	**Teaching Point:**
8	**Teaching Point:** **Comment:**
9	**Comment:** Second click produces the translation - Point out the key words in it to illustrate the method of communication.
10	**Teaching Point:** (Photos of secret writing containers and examples of secret writing used

b7E

(S)

b1
b7E

	during the American Revolutionary War).
11	**Comment:**
12	**Teaching Point:** Many apparently innocent items can be used to hide secret messages. **Comment:**
13	**Teaching Point:** **Comment:**
14	**Teaching Point:** Some relatively simple methods can be highly effective. **Comment:**
15	**Teaching Point:** **Comment:**

b7E

(S)

b1
b7E

16	[redacted] **Teaching Point:** [redacted] b7E **Comments** [redacted]
17,18,19,20,	**Teaching Point:** Acquaint the student with the [redacted] **Comment:** [redacted] b7E
21	**Teaching Point** [redacted] **Comment** [redacted] b7E

22, 23	**Teaching Point:** Acquaint the student with the use of **Comment:**
24	**Teaching Point:** To acquaint the student with **Comment:**
25	**Teaching Point:** To acquaint the student with **Comment:**

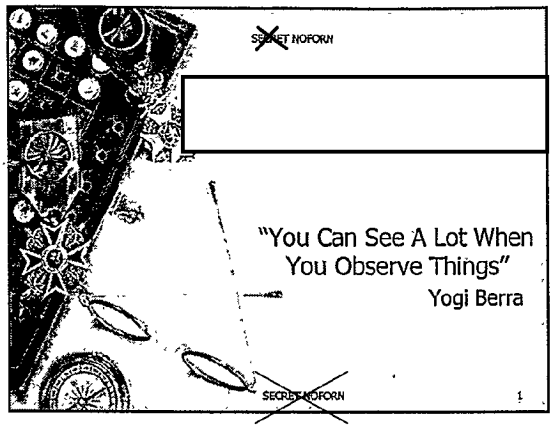
b7E

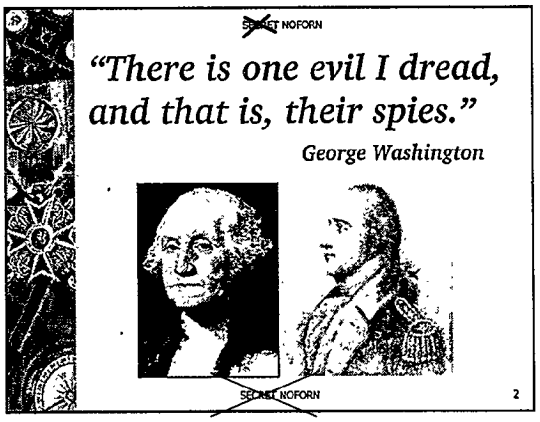
b7E

b7E

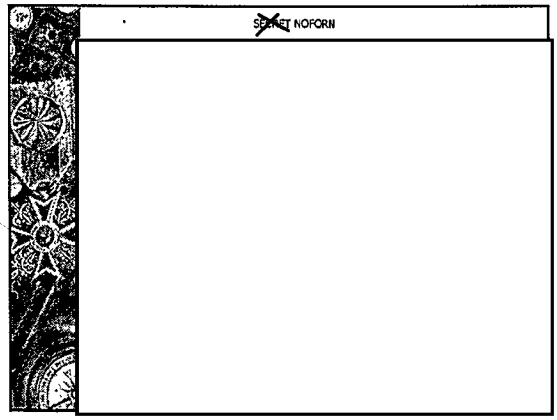
DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

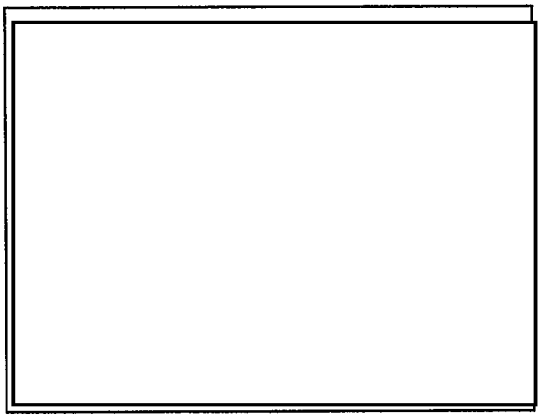




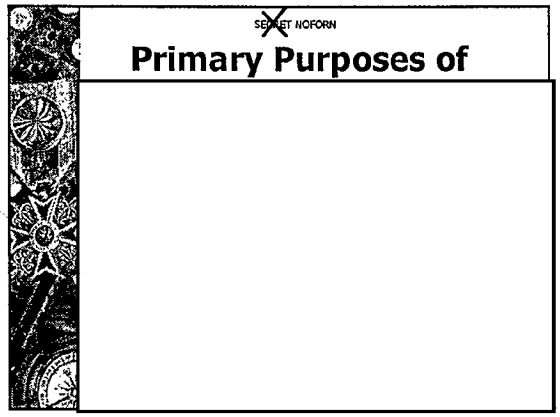
b6
b7C
b7E



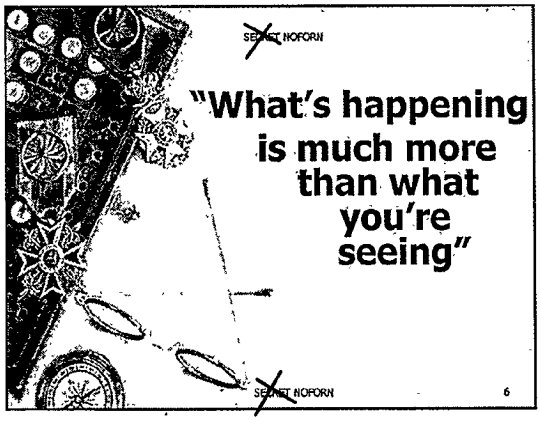
(S)



b1
b7E



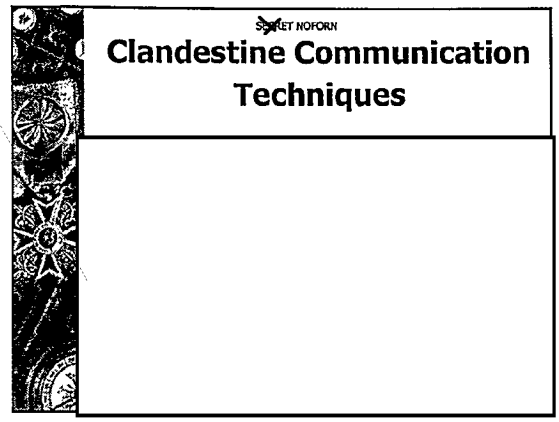
(S)

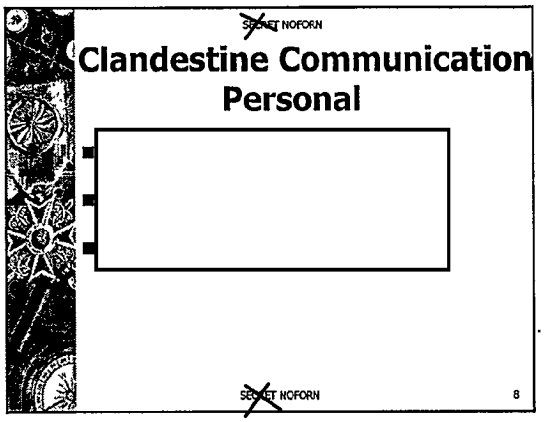


b1
b7E

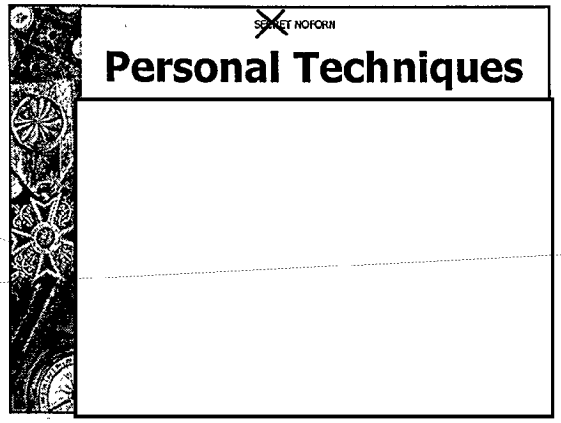


(S)



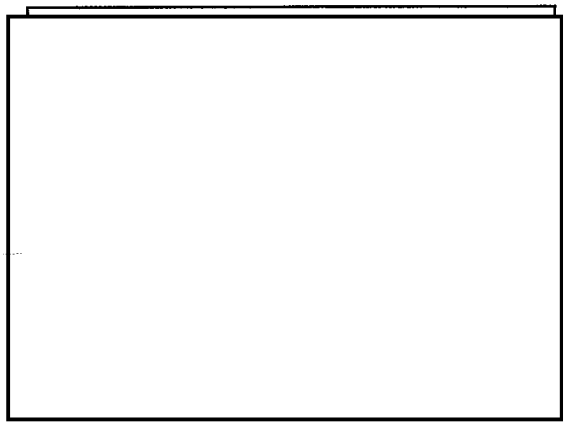


b1
b7E

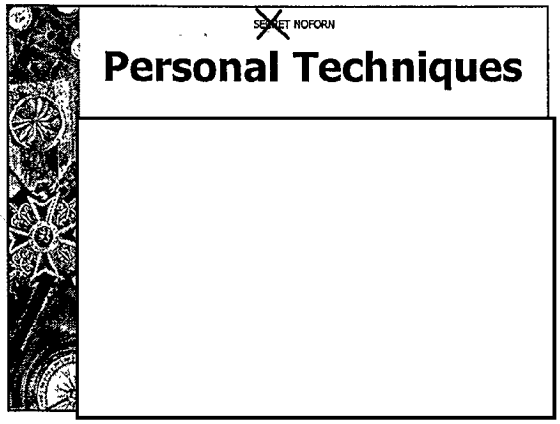


(S)

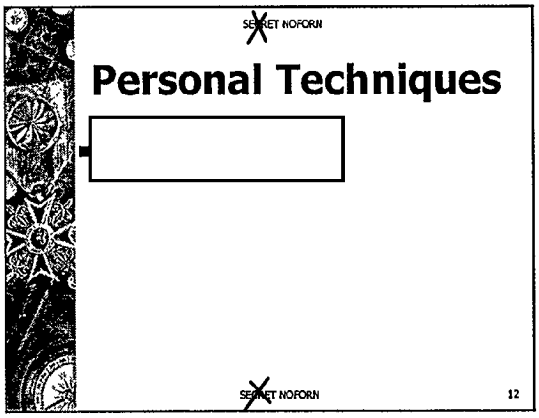
(S)



b1
b7E



(S)



b1
b7E

(S)

(S)

b1
b7E

(S)

(S)

SECRET NOFORN

Personal Techniques

b1
b7E

SECRET NOFORN

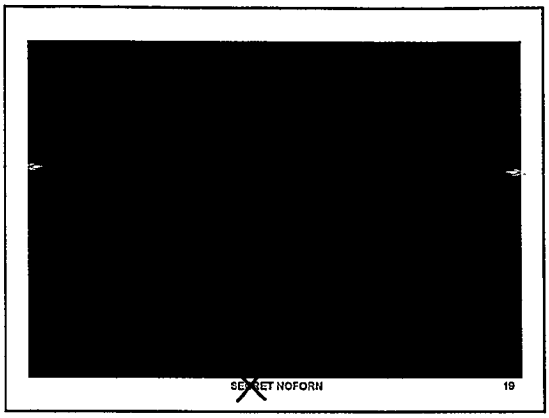
Impersonal Techniques

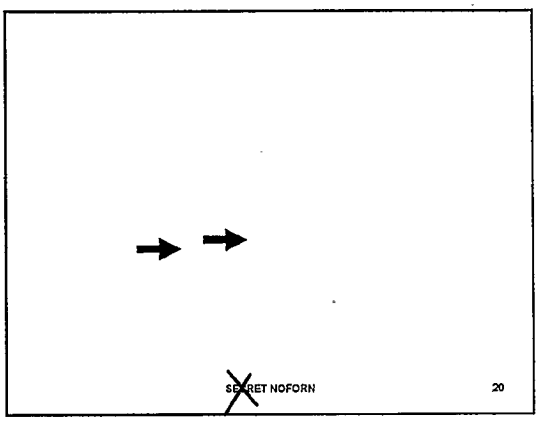
(S)

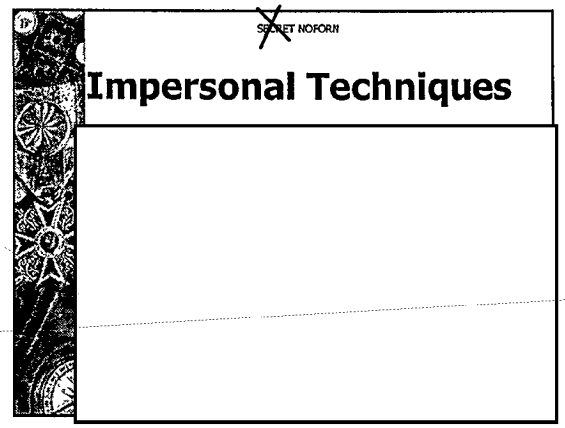
(S)

b1
b7E

SECRET NOFORN 18

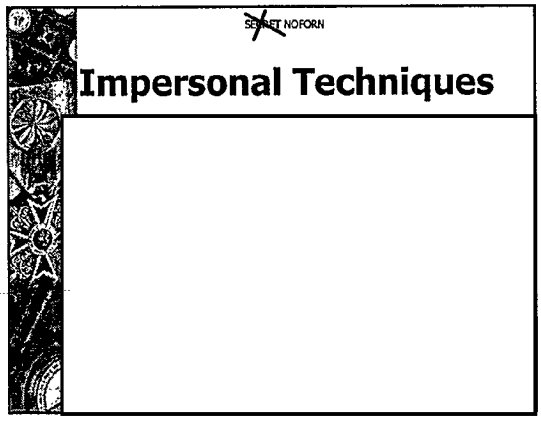




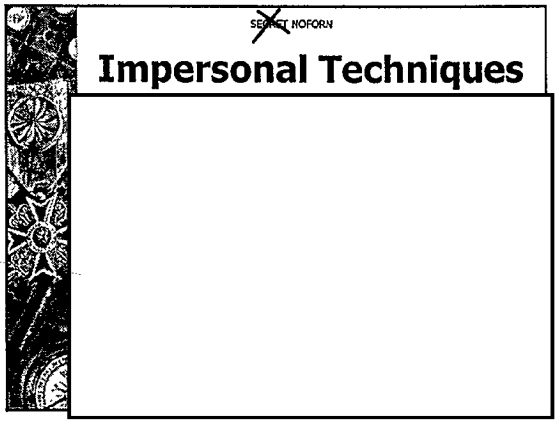


(S)

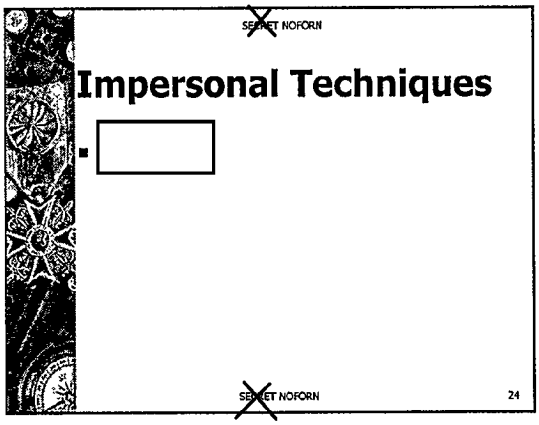
(S)



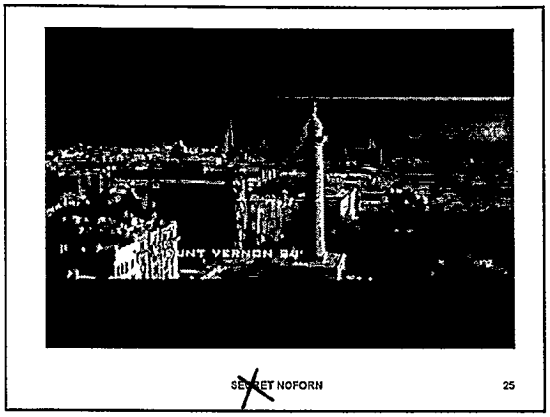
b1
b7E

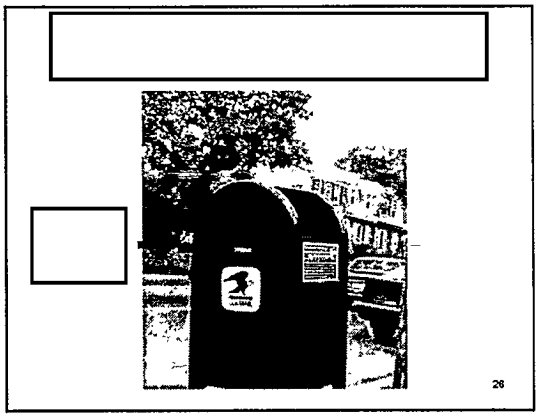


(S)

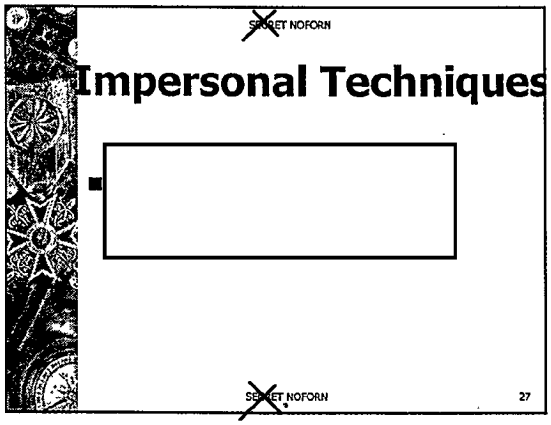


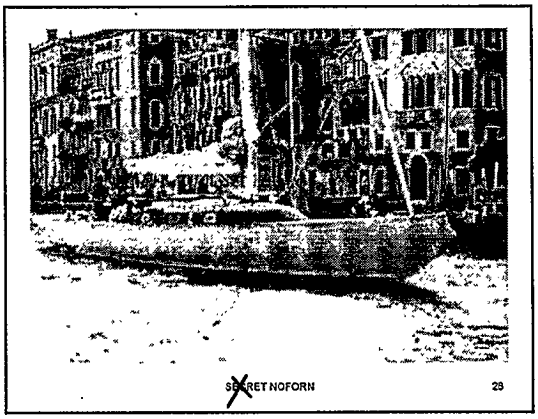
b1
b7E



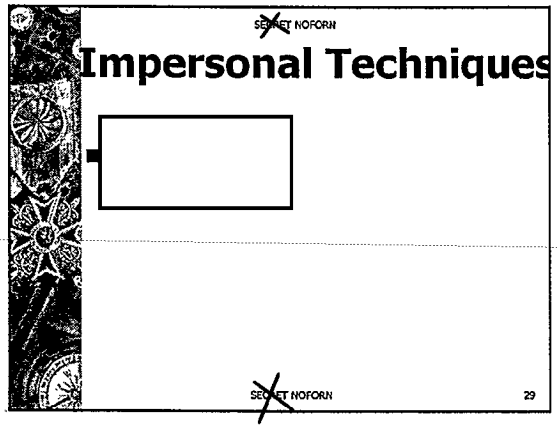


b7E

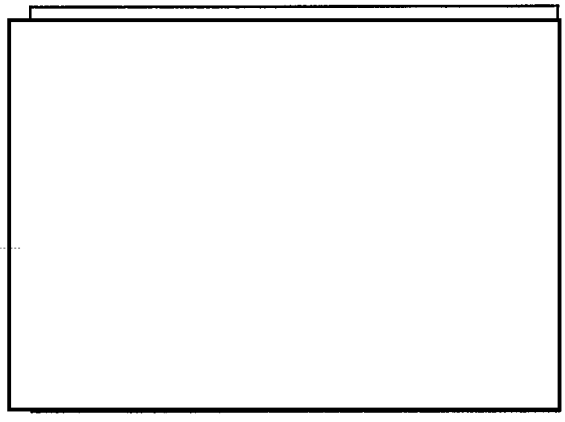




b7E



(S)



b1
b7E

SECRET NOFORN

Impersonal Techniques

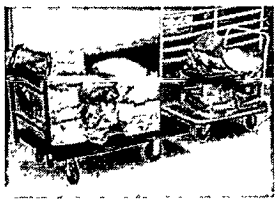
- [redacted]

SECRET NOFORN 31

b7E

Brian Patrick Regan





20,000 pages of classified documents buried in 19 locations in Virginia and Maryland

SECRET NOFORN 32

(S)

SECRET NOFORN

Impersonal Techniques

- [redacted]

SECRET NOFORN 33

b1
b7E

SECRET NOFORN

Impersonal Techniques

- [redacted]

SECRET NOFORN 34

ANNA BELAN MONTES



35

SECRET NOFORN

- [redacted]

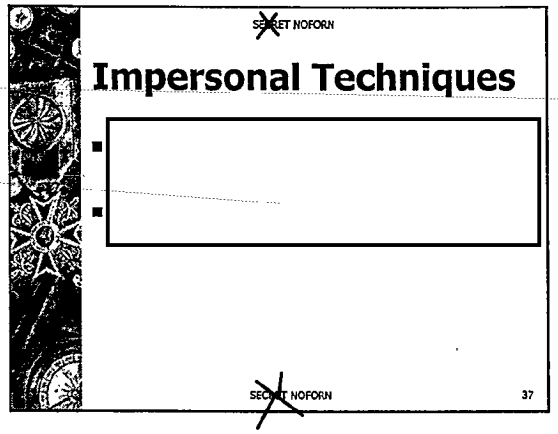
- Carlos and Elsa Alvarez -
- Professors at Florida International University
  - Arrested 2006

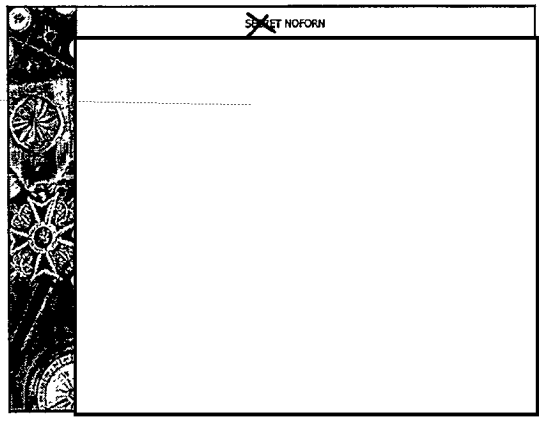
SECRET NOFORN 36

b7E

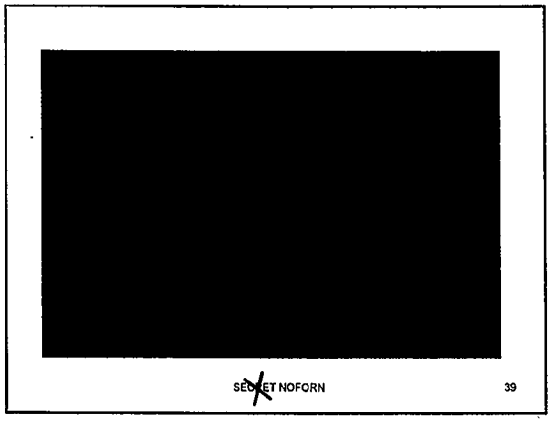
(S)

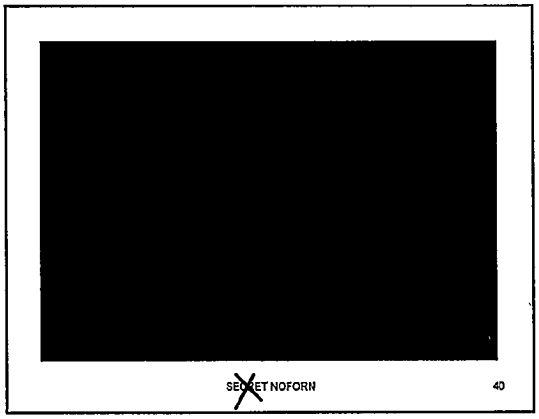
(S)

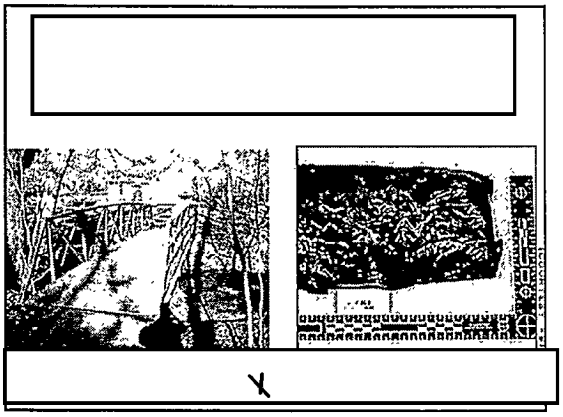


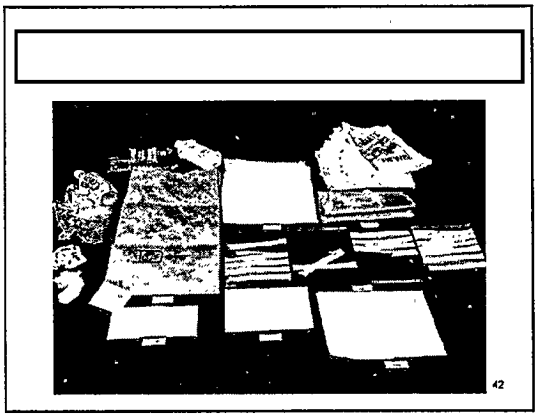


b1
b7E





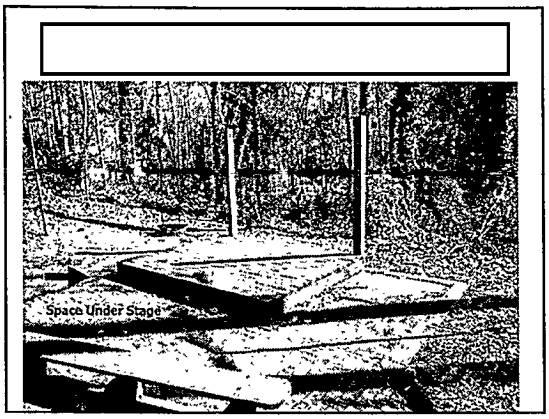




b7E

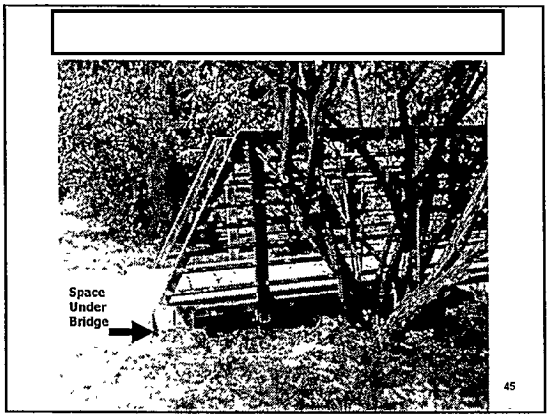
ACLURM032208

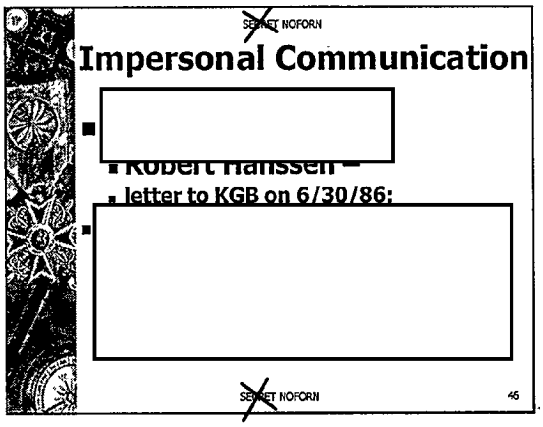
FBI031728



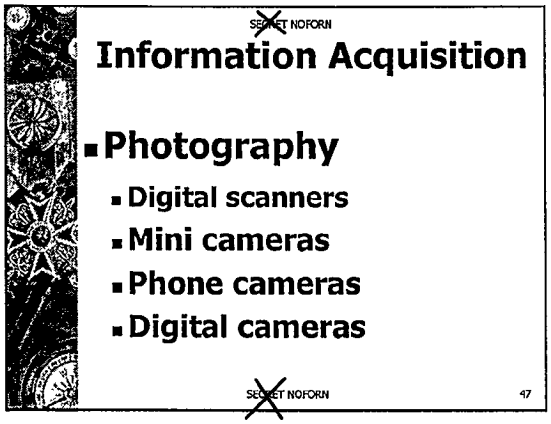


b7E





b7E

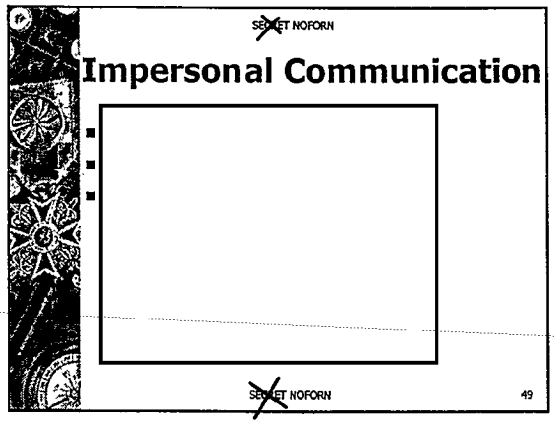




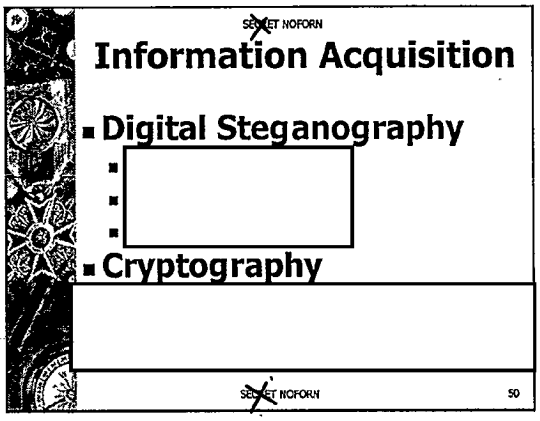
b7E

ACLURM032209

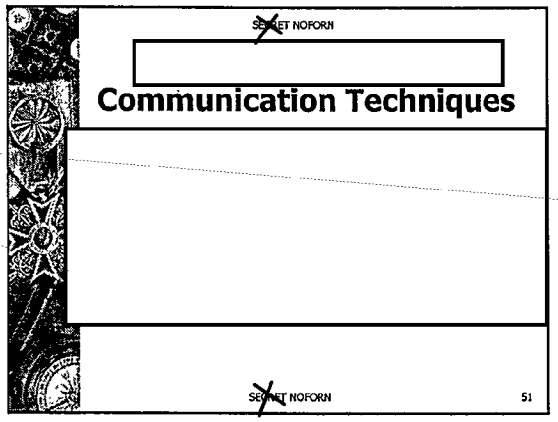
FBI031729



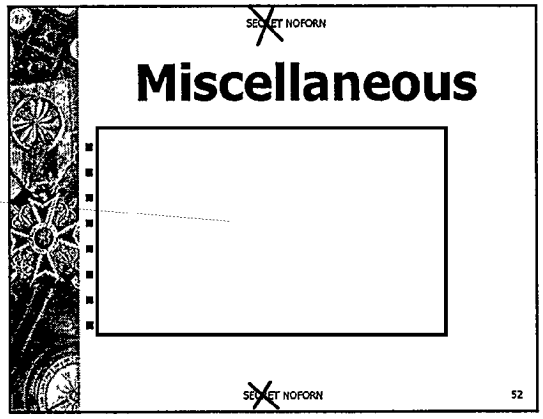
(S)



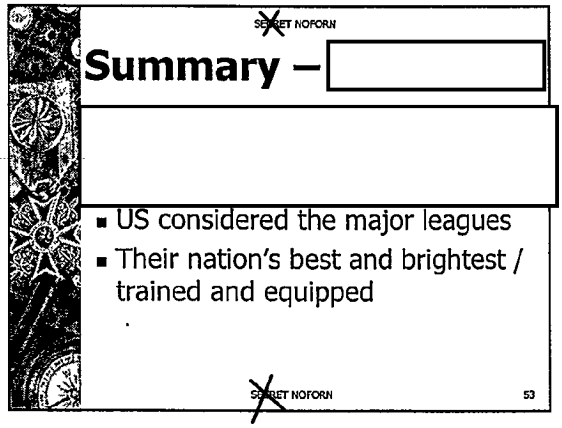
b1
b7E



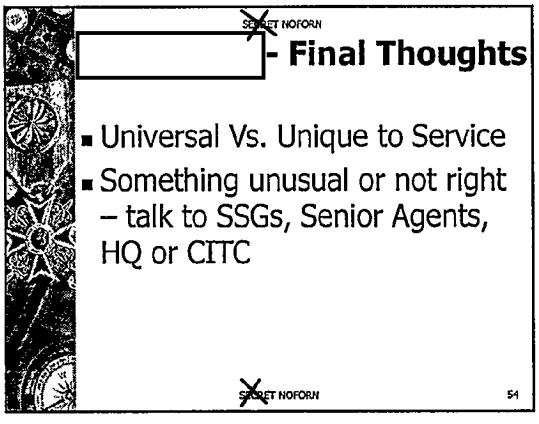
(S)
(S)



b1
b7E



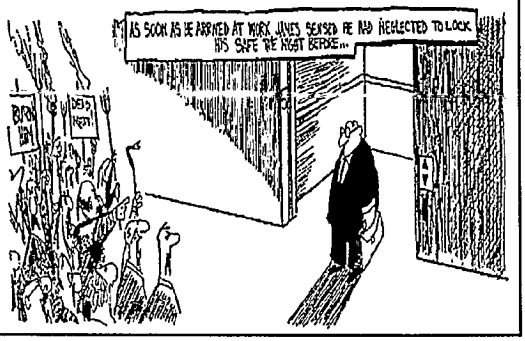
(S)



b1
b7E

ACLURM032210
FBI031730

Questions?



SECRET NOFORN

SECRET NOFORN 56

Techniques

- For Tuesday Practical Exercises
  -
  -
  -
  -
  -
  -
  -
- Foot Emplacement / Retrieval
  -

SECRET NOFORN 57

Act Demonstrations

- Tuesday AM

b7E

SECRET NOFORN 58

Surveillance Practical

- Foot Surveillance Exercise:
  -
- In Afternoon
  -
  -
  -
  -
  -

SECRET NOFORN 59

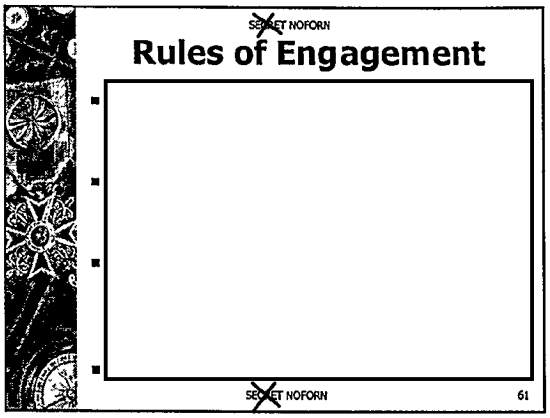
RULES OF ENGAGEMENT

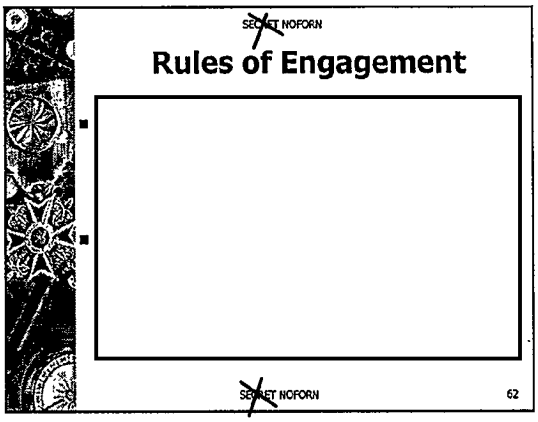
b7E

SECRET NOFORN 60

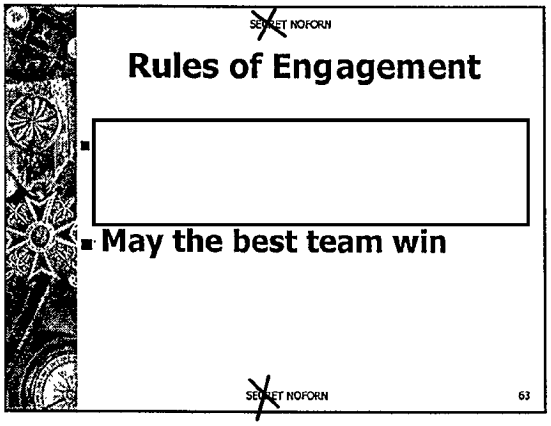
ACLURM032211

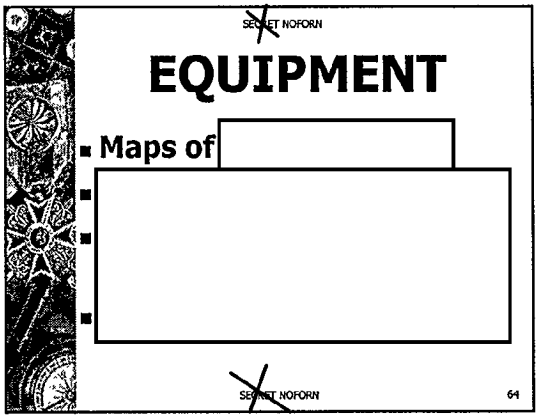
FBI031731



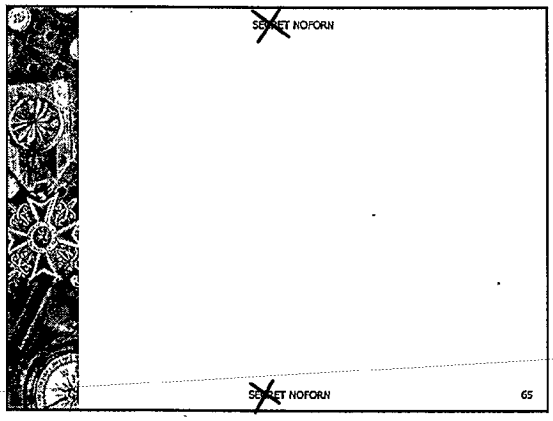


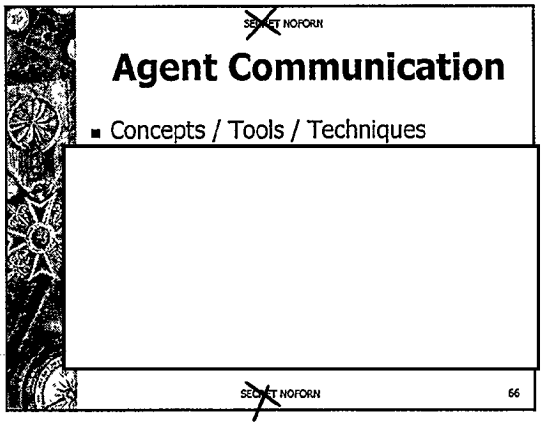
b7E





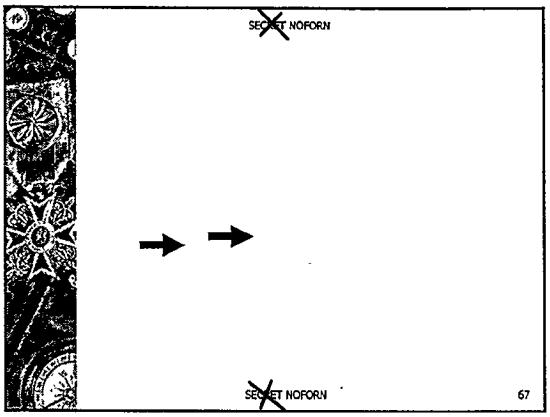
b7E

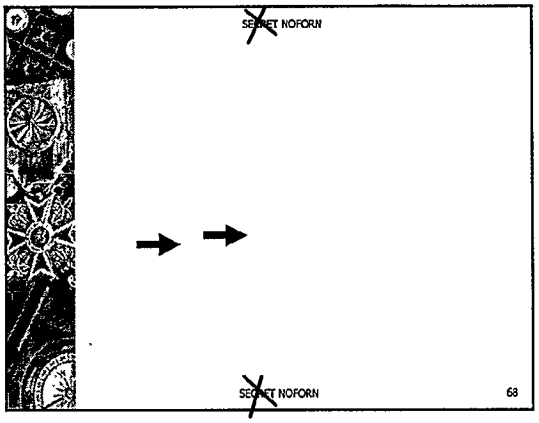




(S)

b1
b7E





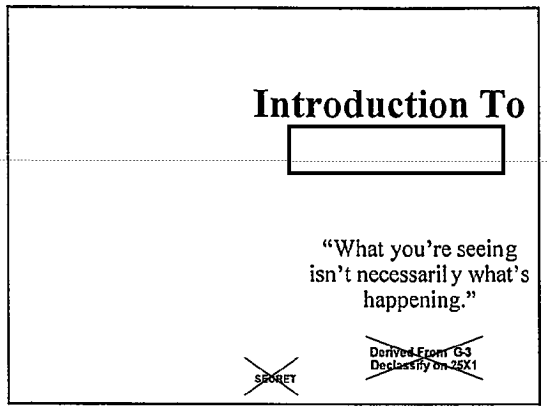
ACLURM032213
FBI031733

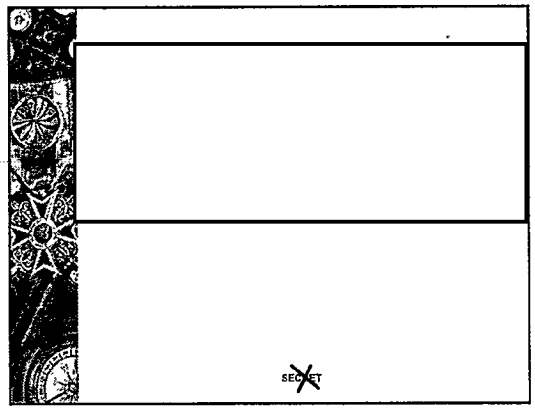
DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

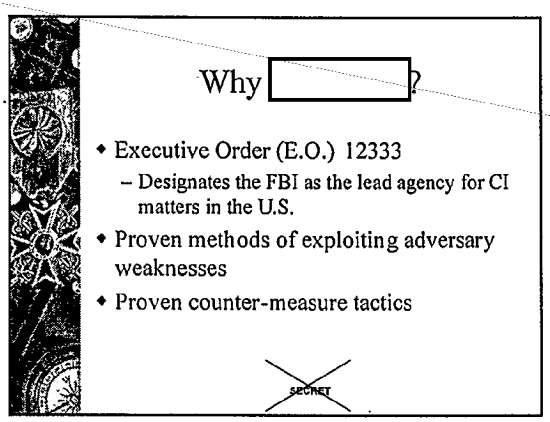
(S)

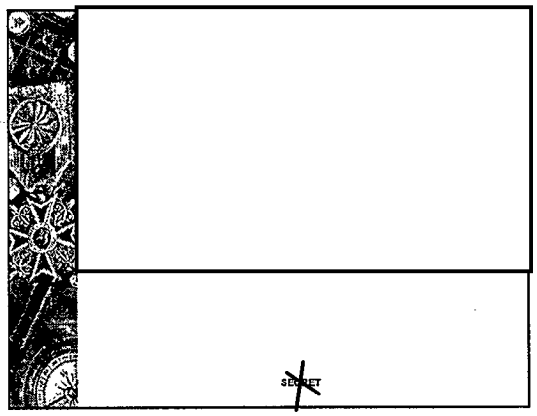




b1
b7E

(S)

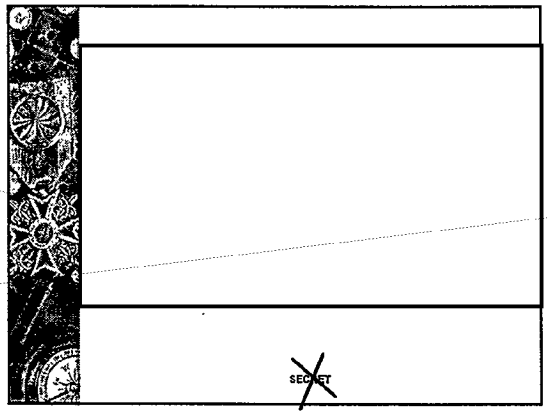


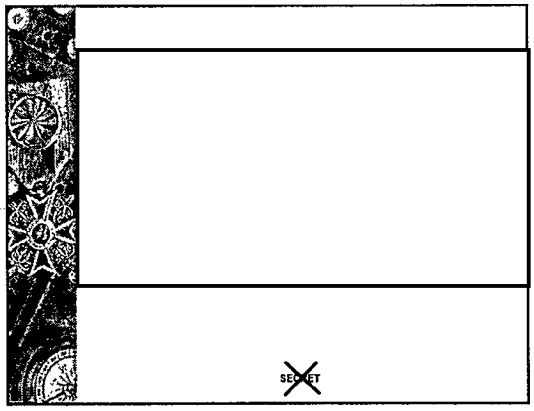


b1
b7E

(S)

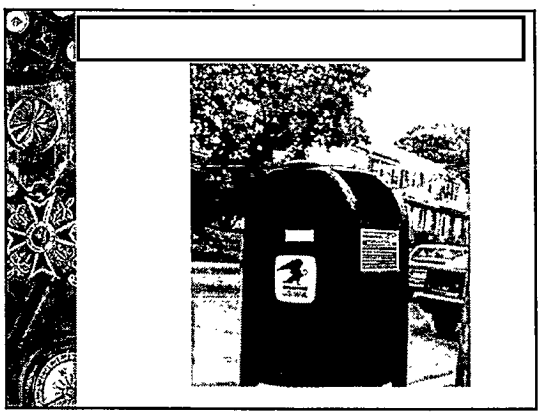
(S)

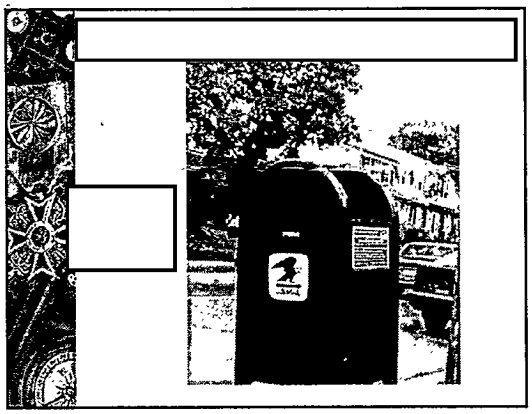




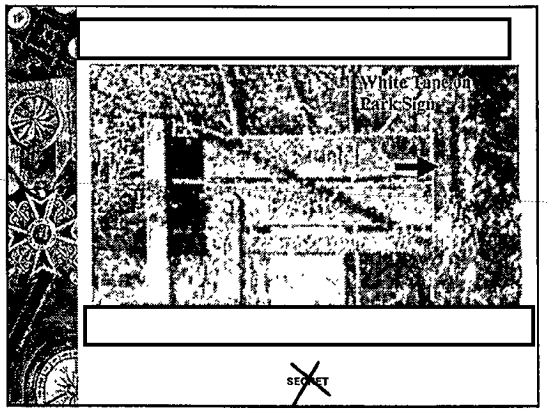
b1
b7E

~~SECRET~~

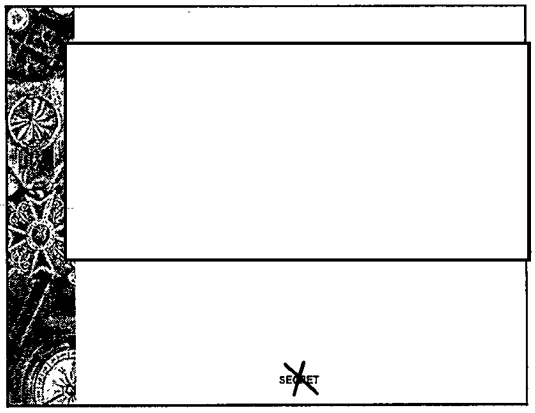




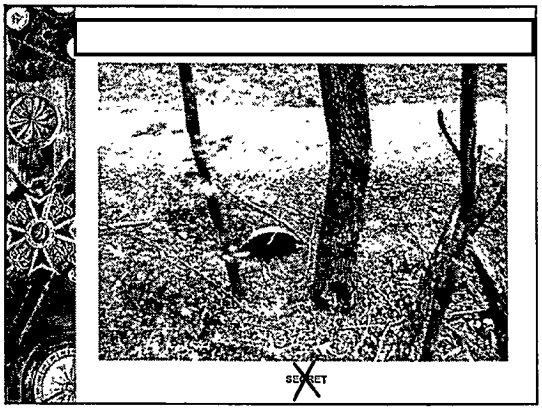
b7E

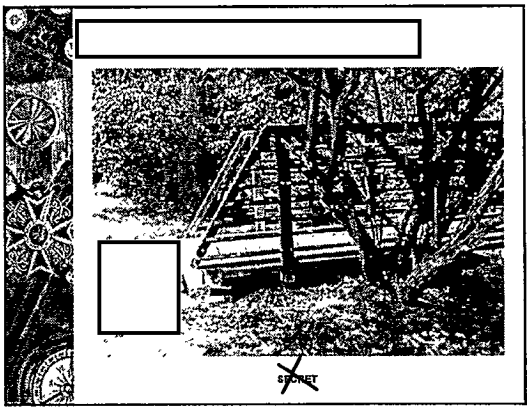


(S)



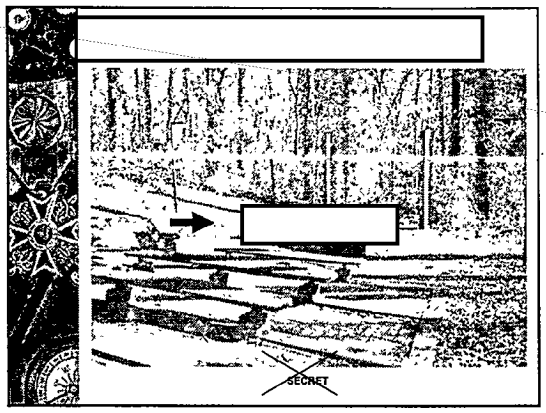
b1
b7E

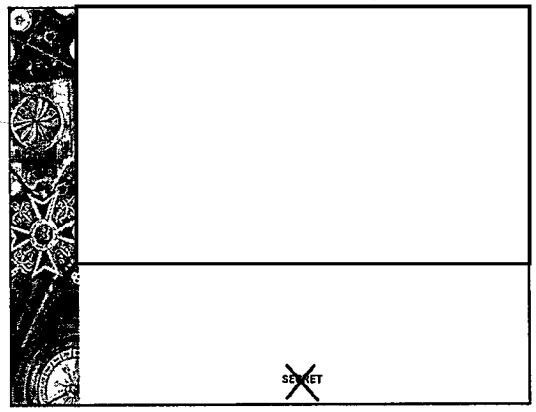




b7E

(S)

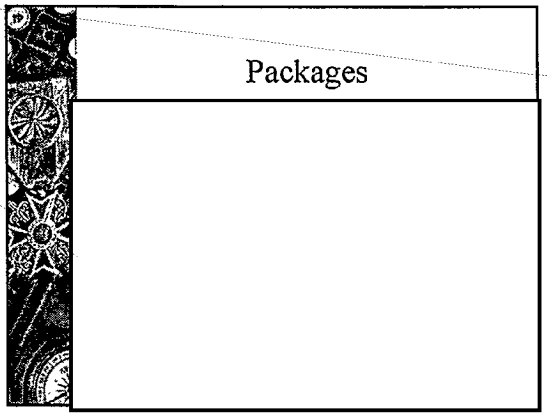


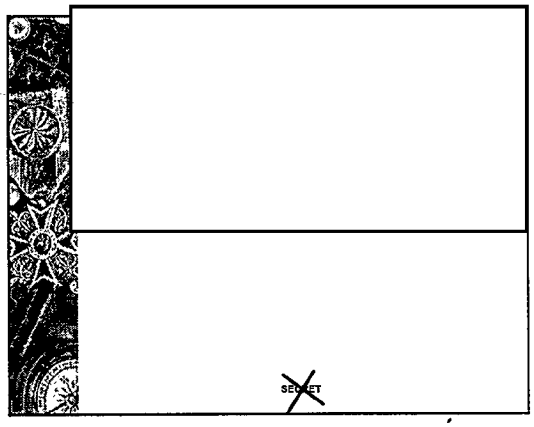


b1
b7E

(S)

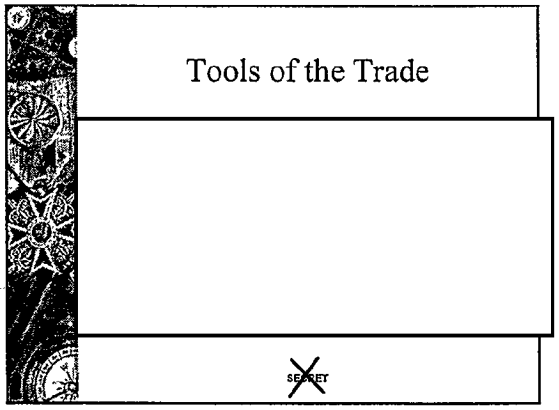
(S)

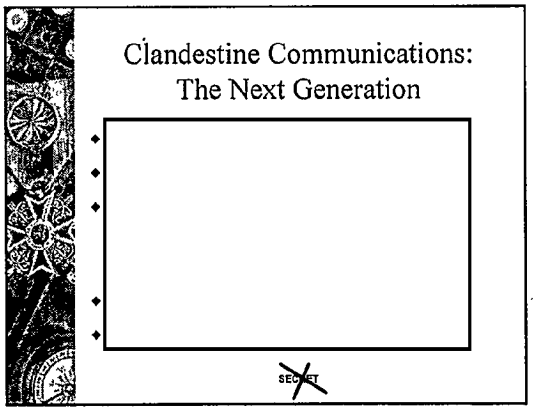




b1
b7E

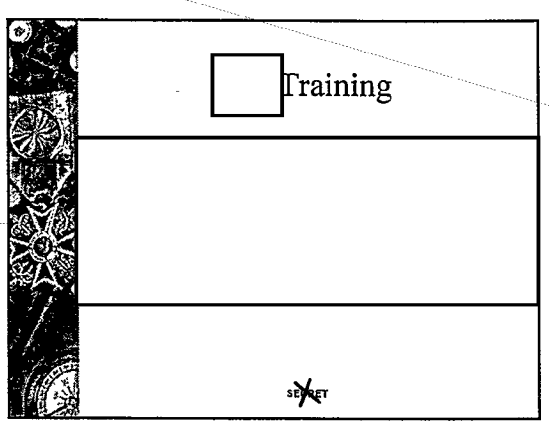
(S)



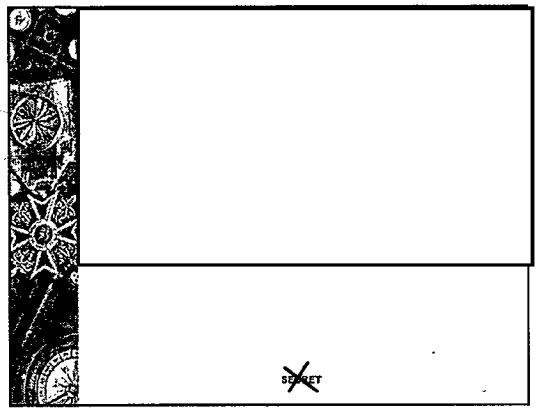


b1
b7E

(S)



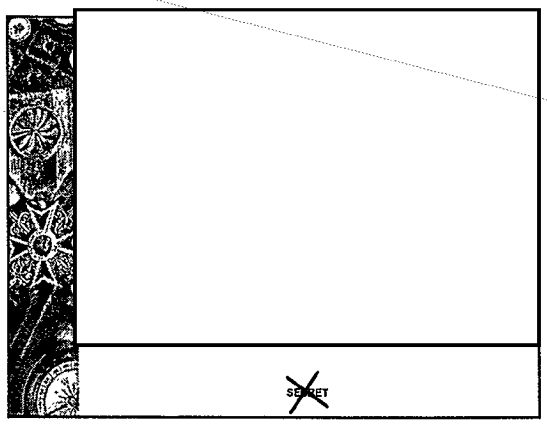
(S)

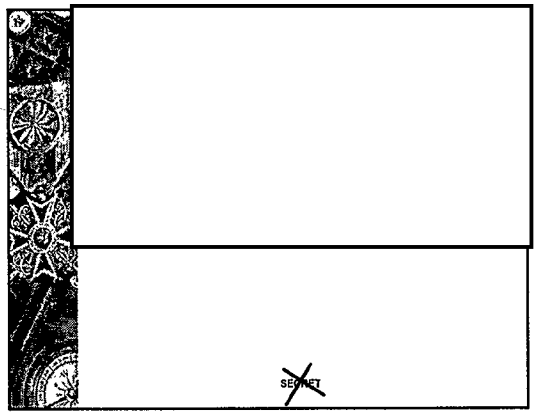


b1
b7E

(S)

(S)

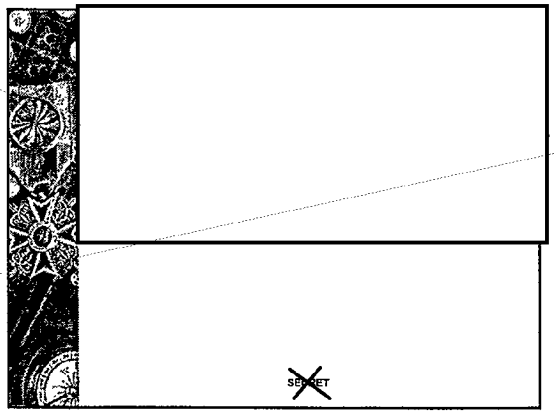


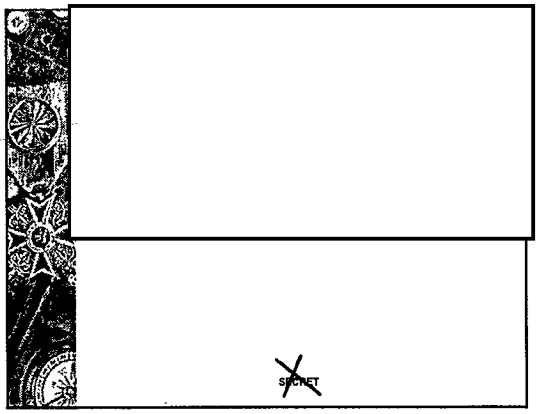


b1
b7E

(S)

(S)

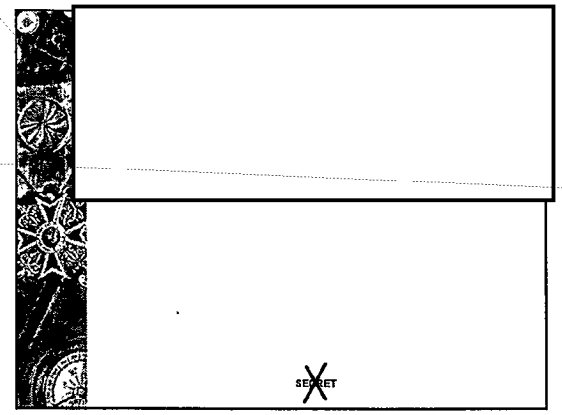


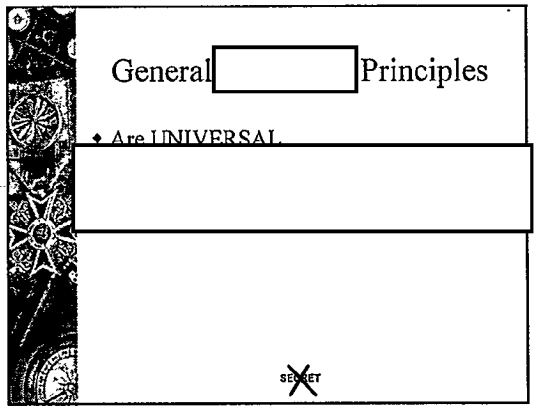


b1
b7E

(S)

(S)

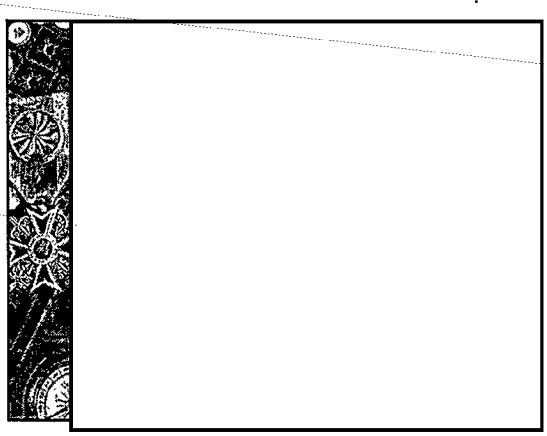


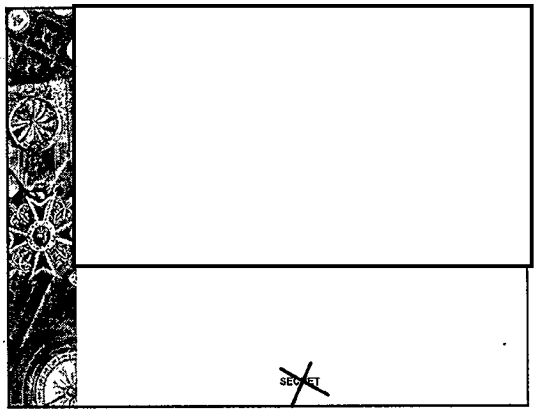


b1
b7E

(S)

(S)



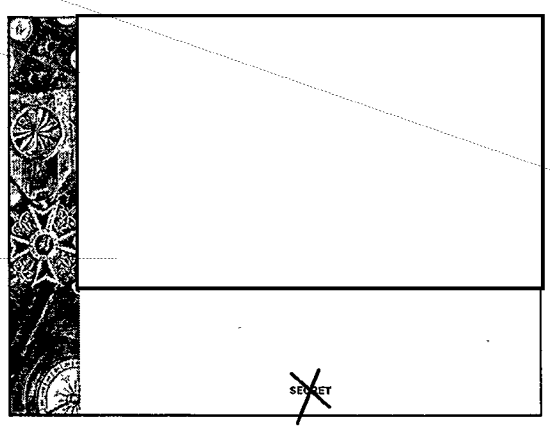


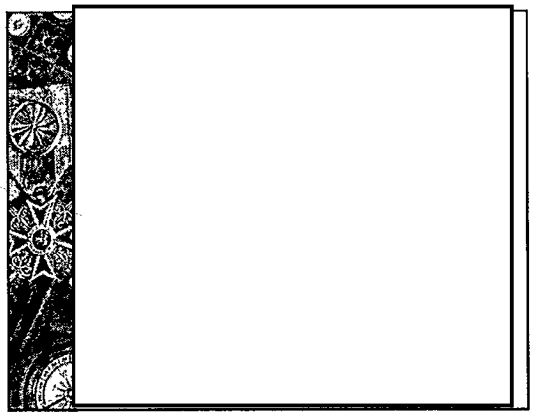
b1
b7E

(S)

(S)

(S)

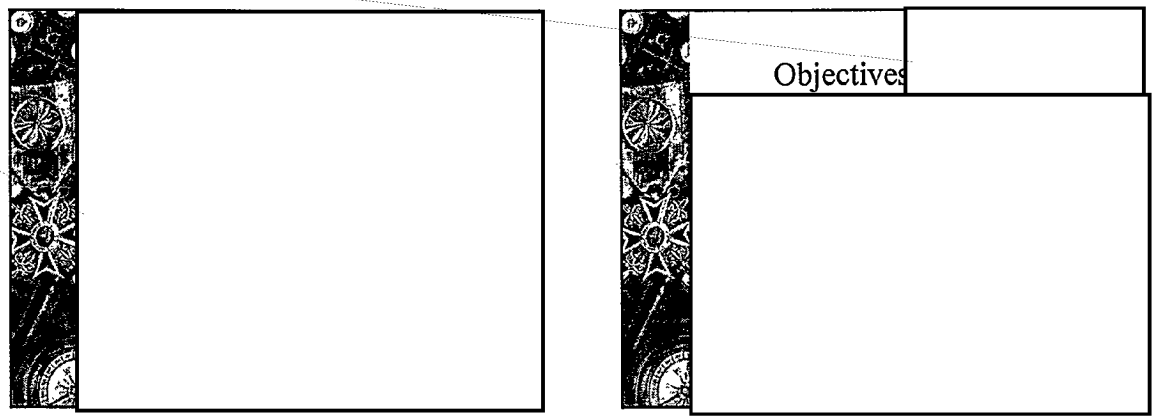




b1
b7E

(S)

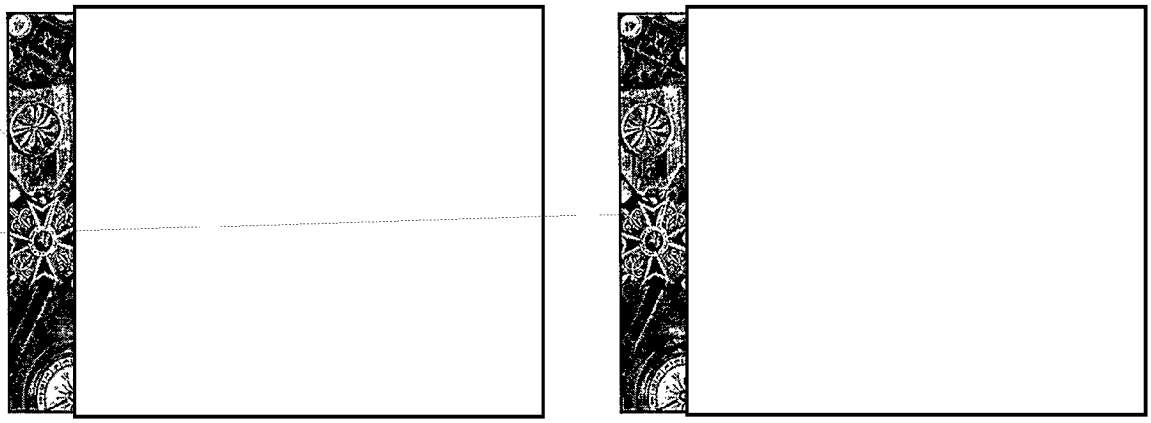
(S)



b1
b7E

(S)

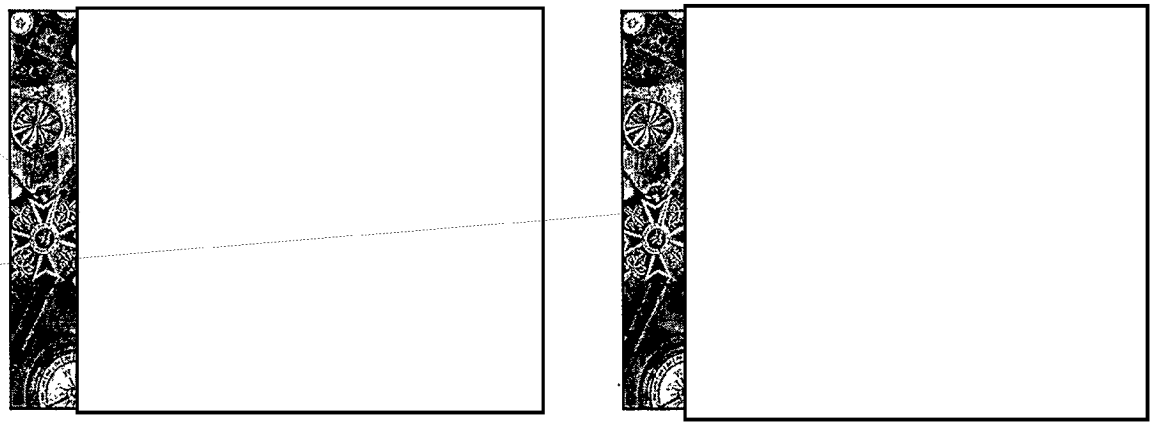
(S)



b1
b7E

(S)

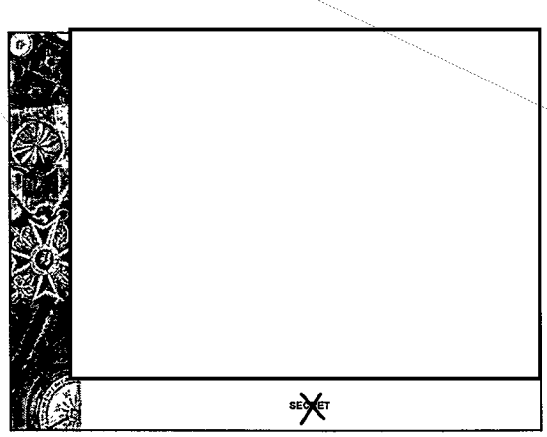
(S)

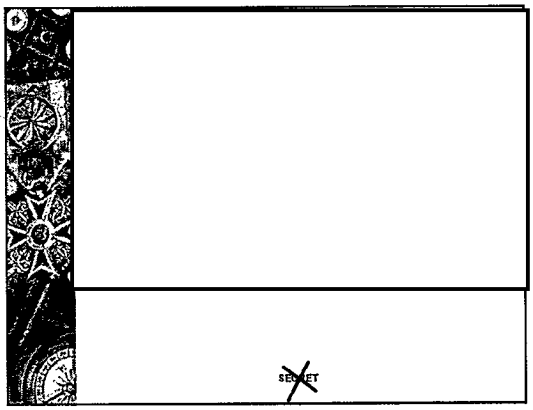


b1
b7E

(S)

(S)

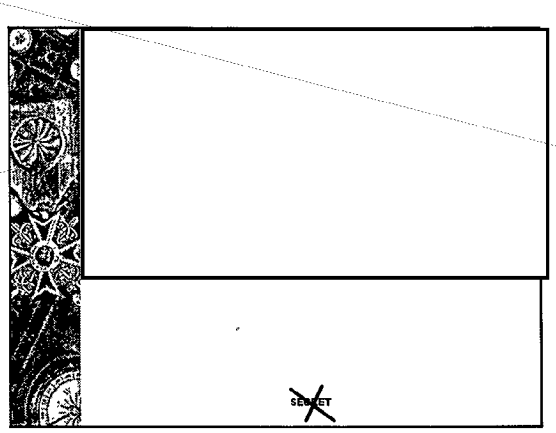


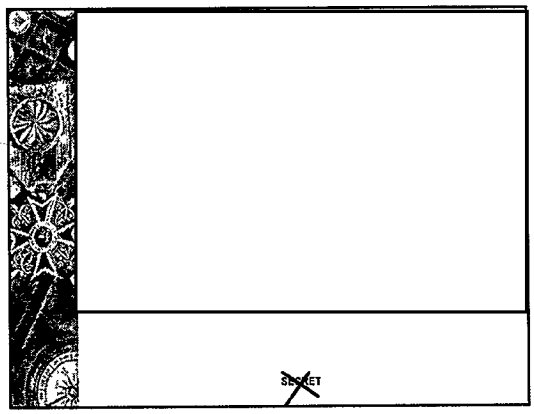


b1
b7E

(S)

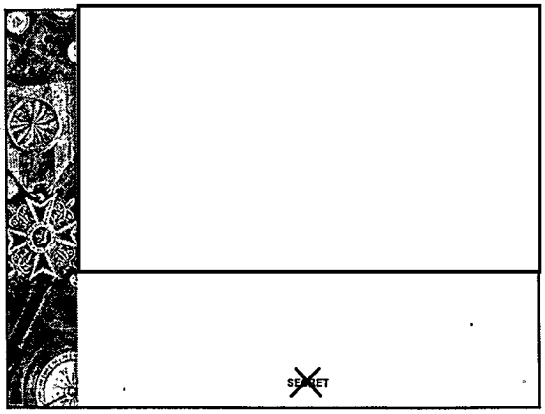
(S)

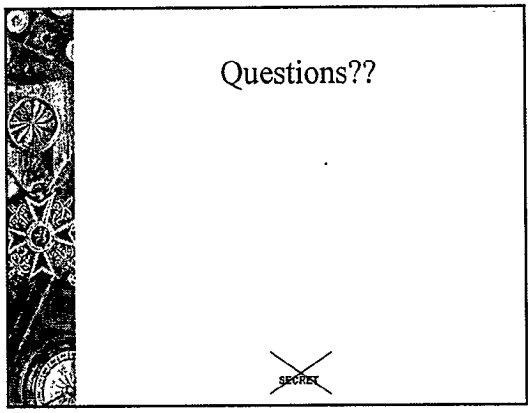




b1
b7E

(S)





b1
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

TOC
unclass
completed

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c,d)
DECLASSIFY ON: 01-11-2037

Course 2A – *Early* [redacted]
June 6, 2006

Federal Bureau of Investigation

Title of Instruction: Early [redacted]

Time of Instruction: Two (2) Hours.

Target Group: FBI Special Agents and other selected personnel.

Instructor: [redacted]

Method of Instruction: Lecture

Additional Information: None

June 6, 2006.

b6
b7C
b7E

Goal: [redacted]

Objective: [redacted]

b7E

Lesson Plan

Early [redacted]

Slide #	*Teaching Points/Comments*
1	Introduction
2	**Teaching Point:** Provide a definition of [redacted] and explain where it fits in understanding an intelligence operation. b1 b7E
(S)	**Comment:** [redacted]
3	**Teaching Point:**
(S)	[redacted]

b7E

Comment:

(S)

b1
b7E

4 **Teaching Point:**

The exchange of information must be

Comment:

5 **Teaching Point:**

Communication can be made in secret writing.

Comment:

Explain the difference between cryptology and cryptography.

6 **Teaching Point:**

Comment:

7 **Teaching Point:**

b7E

8 **Teaching Point:**

Comment:

9 **Teaching Point:**

Secret Writing (SW) still plays a role in spying.

Comment:

Second click produces the translation - Point out the key words in it to illustrate the method of communication.

(S) [redacted]

b1
b7E

(S) [redacted]

10 **Teaching Point:**

Invisible ink may be used to conceal writing.

Comment:

Invisible ink is a substance used for writing, which is either invisible on application, or soon thereafter, and which later on can be made visible by some means. The use of invisible ink is a form of steganography, and has been used in espionage. Other uses may include property marking, hand stamping for readmission, and marking for the purpose of identification in manufacturing.*

* http://en.wikipedia.org/wiki/Invisible_ink

11 **Comment:**

b7E

[redacted]

12 **Teaching Point:**

Many apparently innocent items can be used to hide secret messages.

Comment:

[redacted]

13 **Teaching Point:**

[redacted]

b7E

Comment:

[redacted]

14 **Teaching Point:**

Some relatively simple methods can be highly effective.

Comment:

(S) [redacted]

b1
b7E

15 **Teaching Point:**

[redacted]

Comment:

[redacted]

(Mention Schevchenko case in NY)

16 **Teaching Point:**

[redacted]

Comment:

[redacted]

17 **Teaching Point:**

Acquaint the student with [redacted]

Comment: b7E

[redacted]

18 **Teaching Point**

[redacted]

Comment

[redacted] b7E

19 **Teaching Point:**

Acquaint the student with the use of [redacted]

Comment:

[redacted]

[redacted]

20 **Teaching Point:**

To acquaint the student with [redacted]

Comment:

[redacted]

b7E

21 **Teaching Point:**

To acquaint the student with [redacted]

Comment:

[redacted]

b7E

22 **Teaching Point:**

To acquaint the student with the concept of [redacted]

Comment:

[redacted]

23 **Teaching Point:**

To acquaint the student with the concept of [redacted]

Comment: b7E

(Examples of Ames and Hanssen)

24 **Teaching Point:**

To acquaint the student with the [redacted]

Comment:

(Lonetree and Hanin Cases)

25 **Teaching Point:**

(S) [redacted]

Comment:

[redacted] b1 b7E

26 **Introduction to Segment re Clandestine Electronic Devices**

27 **Teaching Point:**

To acquaint the student with the various different kinds of electronic devices utilized in espionage transactions.

Comment

Describe devices listed in slide.

- Receivers
- Listening Devices

b1
b7E

(S) [redacted]

28 **Teaching Point:**

Radio receivers have been used to provide direction to espionage agents.

Comment

[redacted] b7E

29 **Teaching Point**

Listening devices can be placed surreptitiously to collect information.

Comment

(S) [redacted] b1 b7E

30 **Teaching Point**

(S) [redacted] b1 b7E

Comment

(S) [redacted] b1 b7E

31 **Teaching Point**

Radios have been [redacted]

Comment

(S) [redacted] b1 b7E

[redacted]

32 **Teaching Point**

[redacted]

Comment

[redacted]

(S) b1 b7E

33 **Teaching Point**

[redacted]

Comment

[redacted] b7E

(Photographs and explanation of devices)

34 **Introduction to Segment re Spy Cameras**

35 **Agenda for Section**

See slide.

36 **Teaching Point**

To acquaint the student with the Robot electronic camera which was used in a number of espionage operations.

Comment

[redacted]

37 **Comment**

[redacted]

38 **Teaching Point**

To acquaint the student with [redacted]

Comment

[redacted]

b7E

39 - 41 **Teaching Point**

To acquaint the student with [redacted]

Comment

[redacted]

42 - 44 **Teaching Point**

To acquaint the student with [redacted]

Comment

[redacted]

b7E

45 **Segment re Concealed Devices**

46 **Teaching Point**

A variety of common devices found in many homes or offices have been used to secrete intelligence.

Comment

A variety of common, everyday devices have been utilized by intelligence services to enable their agents to conceal information and equipment. Several of these devices appear on this and the following slides.

47 **Comment**

[redacted]

48 **Comment**

Another concealment for a camera – [redacted]

49 **Teaching Point**

The situation drives the design of the concealment.

Comment

[redacted] concealment device. b7E

50 **Comment**

[redacted]

51 **Comment**

Again, a common item used to conceal something used in espionage.

52 **Comment**

Again, a common item used to conceal something used in espionage.

53 **Comment**

Everyone has one or more of these.

54 **Comment**

[redacted] b7E

55 **Introduce Segment re [redacted] is Countered**

56 **Teaching Point**

(S) [redacted]

Comment

The methods that will be discussed are listed on the slide. b1 b7E

57 **Teaching Point**

(S) [redacted]

Comment

(S) [redacted]

58 **Teaching Point**

(S) [redacted]

Comment

(S) [redacted] b1 b7E

Mention also:

[redacted]

59 **Teaching Point**

[redacted]tect

b7E

Comment

[redacted] countermeasures are as varied as are CI Officers.

60 **Teaching Point**

[redacted]

Comment

Describe the Verona Case and what it revealed about Soviet intelligence operations and activities in the US. Julius and Ethel Rosenberg were guilty.

Point out how difficult it is today to break encrypted messages.

b7E

61 **Teaching Point**

[redacted]

Comment

[redacted]

62 **Teaching Point**

Video may be used to surveil an espionage meeting, [redacted]

[redacted]

b7E

Comment

Generally, video is an important technique when CI has an idea of where an activity may occur. Then the placement of video cameras may collect intelligence or evidence to be used in a prosecution.

63 **Comment**

[redacted]

64 **Teaching Point**

(S) To acquaint the student with the technique of surveillance [redacted]

[redacted]

b1
b7E

Comment

(S) [redacted]

65 **Teaching Point**

To acquaint the student with the technique of [redacted]

Comment

b7E

[redacted]

66 **Training Point**

b7E

(S) [redacted]

Comment

DISCUSS THE BENEFITS OF RECRUITMENT citing cases involving Oleg Gordievsky, Boris Yuzhin, Kim Philby, and Vasili Mitrokhin. Discuss the impact of the Robert Hanssen case on the FBI and of the Aldrich Ames case on the CIA.

b1
b7E

(S) [redacted]

Photos are of Arkady Shevchecnko, Mitrokin, Philby, Guy Burgess, Donald Maclean, Ed Howard, Ames, Hanssen, Felix Block, Dmitri F. Polyakov, Valeri Martynov, and Sergei Motorin .

Criterion Test Questions:

(S) [redacted]

b1
b7E

Test Answers:

(S) [redacted] b1 b7E

(S) [redacted]

Equipment:

Equipment/Aids for Instructor: Power Point Projector and VHS

Equipment/Aids Required for Instructor: Power Point projector and VCR

Equipment/Aids Required for Students: None.

Power Point Slides or Overheads: Power Point Slides.

Handouts: Yes.

Bibliography:

Ronald Kessler. *Moscow Station*. New York: Charles Scribner's Sons, 1989.

Ronald Kessler. *The Spy in the Russian Club*: Charles Scribner's Sons, 1990.

Sherry Sontag and Christopher Drew. *Blind Man's Bluff*. New York: Public Affairs, 1998.

David Wise. *Spy*. New York: Random House, 2002.

Course 2B – *Contemporary* [redacted]
June 6, 2006

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Federal Bureau of Investigation

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

Title of Instruction: Contemporary [redacted] b6 b7C b7E

Time of Instruction: Two (2) Hours

Target Group: FBI Special Agents and other selected personnel

Instructor: [redacted]

Method of Instruction: Lecture

Additional Information: None

June 6, 2006.

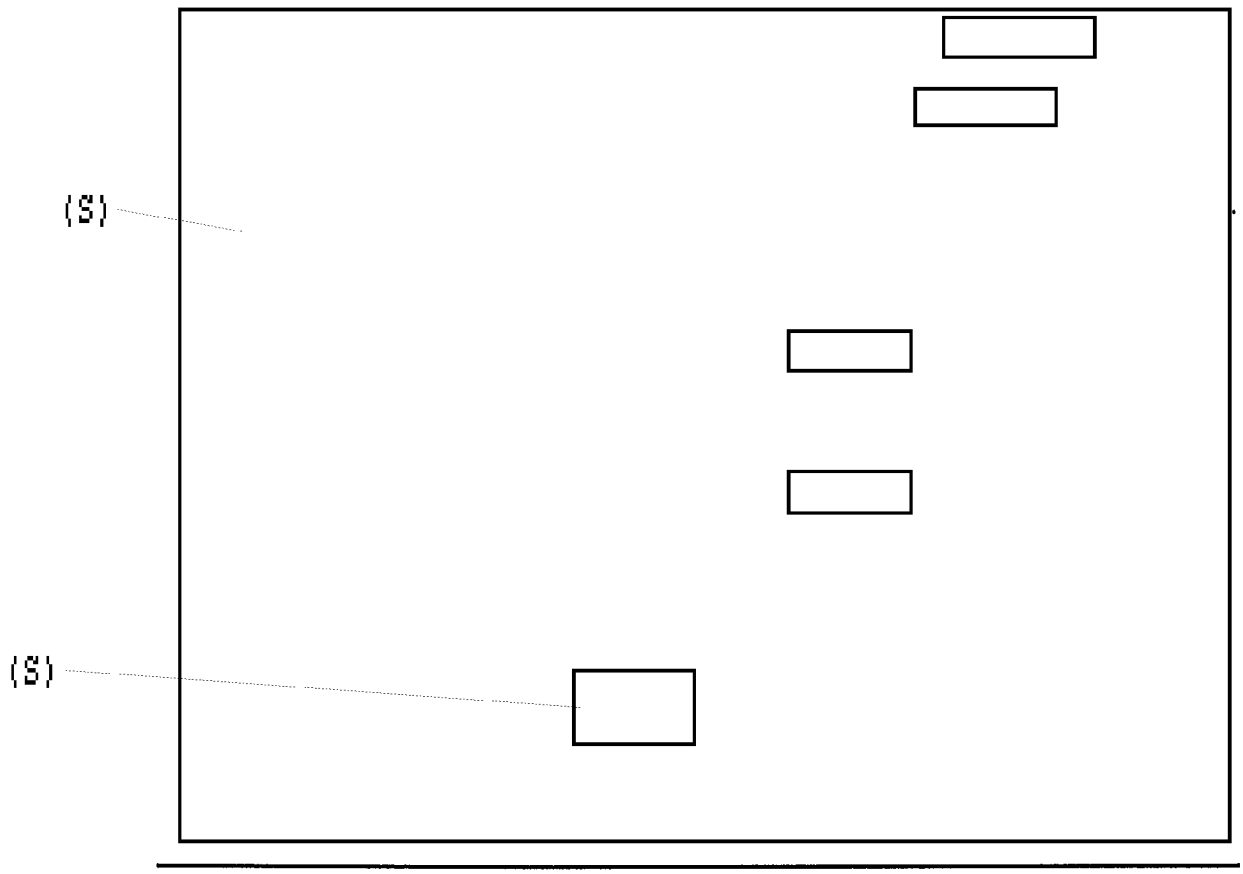
(S) **Goal:** [redacted]

Objective [redacted] b1 b7E

(S) [redacted]

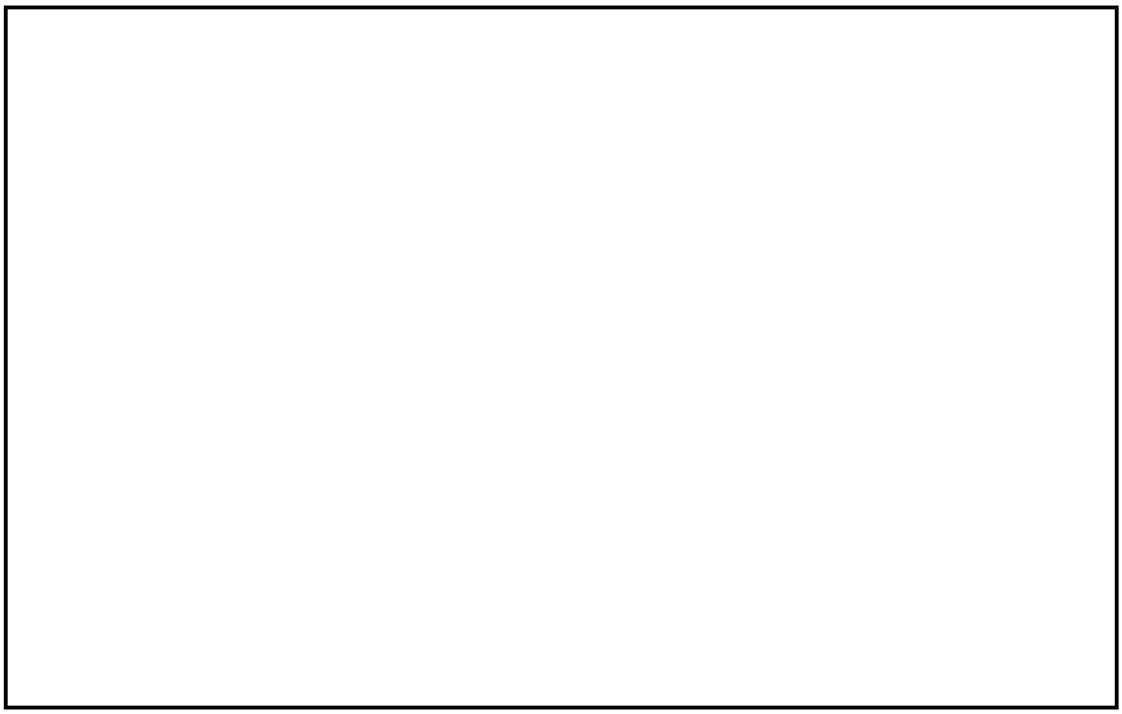
Criterion Test Questions:

[redacted] b7E



b1
b7E

Test Answers:



b7E

(S) [redacted]

(S) [redacted]

b1
b7E

Equipment:

Equipment/Aids for Instructor: Power Point Projector and VHS

Equipment/Aids Required for Instructor: Power Point projector and VCR

Equipment/Aids Required for Students: None.

Power Point Slides or Overheads: Power Point Slides.

Handouts: Yes.

Bibliography:

Ronald Kessler. *Moscow Station*. New York: Charles Scribner's Sons, 1989.

Ronald Kessler. *The Spy in the Russian Club*: Charles Scribner's Sons, 1990.

Sherry Sontag and Christopher Drew. *Blind Man's Bluff*. New York: Public Affairs, 1998.

David Wise. *Spy*. New York: Random House, 2002.

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~For Official Use Only~~

CITC OUTREACH BRANCH

The CITC Outreach Branch supports three functions that span beyond traditional Counterintelligence training in the FBI, to include expanded and new CI training for agent and non agent personnel, CI training and awareness for members of the Intelligence Community (IC), and added liaison with the IC.

CITC TRAINING AT THE

SSG Training: Training new SSG members has been a function of the Outreach Branch for many years. In January 2007 we began to transition the training to familiarize the personnel with CITC training responsibilities. The training materials CITC provided to include newly-updated presentations and lesson plans for the following:

in

b6
b7C
b7E

This involves approximately 12 hours of training and is taught on demand for
The POC for this training is

(S)

b1
b7E

~~For Official Use Only~~

~~SECRET~~

ACLURM032243

(S) [redacted] POC is SSA [redacted]

b1
b6
b7C
b7E

CITC TRAINING PROVIDED TO OUTSIDE AGENCIES

CITC Outreach provides training to: the Interagency Training Center (ITC), the Counterintelligence Field Activity (CIFA), the Defense Intelligence Agency (DIA), the Intelligence Community Officer Course (ICOC) a joint IC course, the National Geospatial-Intelligence Agency (NGA), the United States Secret Service, and the National Counterintelligence Executive (NCIX).

(S) **ICOC Training**: CITC Outreach provides training for the Intelligence Community Officer course at [redacted] Reston, VA. This course is for GS-15 and above in the USIC. The one-hour training module is entitled NSB and Federal Partners and provides an overview of NSB and how the FBI works with our Federal Partners. Prior to 2006, this FBI was not provided a slot for this teaching, but the Outreach team requested and became a regular part of this instruction. The training takes place every four-five weeks. The POC for this training is [redacted]

b1
b6
b7C
b7E

(S) **ITC Training**: CITC Outreach provides training for the ITC [redacted]

(S) The one hour training module is entitled Omega 4 and provides [redacted] with an understanding of what strategy and resources the FBI would apply to them if they were trying to operate in the U.S. The ITC training facility is located in located in [redacted] POC for this training is SSA [redacted] detailed to the ITC, [redacted] Bill Kline, ITC Director, [redacted]

b1
b6
b7C
b7E

CIFA training - CITC Outreach works closely with CIFA's Joint Counterintelligence Training Academy **(JCITA)**, on their CI Staff Officer's Course. The one hour training block is entitled NSB and Federal Partners. It provides an overview of NSB and how the FBI works with our Federal Partners. The training site is [redacted] POC for this training is [redacted] Course Director, JCITA, [redacted]

b6
b7C
b7E

DIA training - CITC Outreach provides training for the Joint Military Intelligence

Training Center (**JMITC**), part of Defense Intelligence Agency (DIA), at their facility at [redacted] and once a year to a Combatant Command. The one hour training block was entitled NSB and Federal Partners. This is the same block provided to DIA personnel at [redacted] POC for this training is [redacted] JMITC, [redacted] b6 b7C b7E

COUNTERINTELLIGENCE YESTERDAY AND TODAY course
CITC contracted for and reviewed a pilot of 38 hours of unclassified training blocks on the importance of counterintelligence to national security. In June 2005, CITC Outreach personnel assisted in securing a five-year contract with four companies and out of those five companies, MPRI was awarded the contract to produce these blocks of CI training. In FY07 itis planned to hold the course in Boston and Cincinnati field offices. b6 b7C
POC for this training is [redacted] (cell), and [redacted] office).

Technology Transfer DVD
(S) CITC Outreach Branch commissioned a DVD of a fictional technology transfer case investigation. The DVD is a starting point to provide training regarding [redacted] The DVD will be placed on the Virtual Academy and be followed by blocks of specialized instruction. b1 b6 b7C b7E
POC for this training is SSA [redacted] POC at the Biograph is [redacted].

Additional POCs who have intermittently worked with Outreach Branch are:

(S) [redacted]

(S) [redacted] b1 b6 b7C b7E

Recruitment Center

[redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

October

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2 Managing CI Investigation & Operations 0701 [redacted] - QT	3 Managing CI Investigation & Operations 0701	4 Managing CI Investigation & Operations 0701	5 Managing CI Investigation & Operations 0701	6 Managing CI Investigation & Operations 0701	7
8	9 Holiday	10	11	12	13	14
15	16 CIOPS 0701 QT [redacted]	17 CIOPS 0701	18 CIOPS 0701	19 CIOPS 0701	20 CIOPS 0701	21
22	23 CIOPS 0701 Week 2	24 CIOPS 0701	25 CIOPS 0701	26 CIOPS 0701	27 CIOPS 0701	28
29	30 CIOPS 0701 Week 3	31 CIOPS 0701				

b6
b7C

2006

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/EAW/STP/bls

November

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1	2	3	4
5	6 CIOPS 0701 Week 4	7 CIOPS 0701	8 CIOPS 0701	9 CIOPS 0701	10 Holiday	11
12	13 CI Espionage Course 0701 OT	14 CI Espionage Course 0701	15 CI Espionage Course 0701	16 CI Espionage Course 0701	17 CI Espionage Course 0701	18
19	20	21	22	23 Thanksgiving	24	25
26	27 CI Yesterday and Today	28 CI Yesterday and Today	29 CI Yesterday and Today	30 CI Yesterday and Today	CI Yesterday and Today	

b6
b7C

b6
b7C

2006

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

December

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1 Counterproliferation for CI Investigors 0701	2
3	4 CI [redacted] Course 0701 QT [redacted]	5 CI [redacted] Course 0701	6 CI [redacted] Course 0701	7 CI [redacted] Course 0701	8 CI [redacted] Course 0701	9
10	11 CI [redacted] Operations Course QT 0701 [redacted]	12 CI [redacted] Operations Course 0701	13 CI [redacted] Operations Course 0701	14 CI [redacted] Operations Course 0701	15 CI [redacted] Operations Course 0701	16
17	18	19 WMD and CP Seminar [redacted]	20 WMD and CP Seminar [redacted]	21 WMD and CP Seminar [redacted]	22	23
24	25 Holiday	26	27	28	29	30
31						

2006

b6 b7C b7E

b6 b7C b7E

b6 b7C b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

January

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1 Holiday	2	3	4	5	6
7	8	9 CP Regional Seminar [redacted]	10 CP Regional Seminar [redacted]	11 CP Regional Seminar [redacted]	12	13
14	15 Holiday	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30 ICOC 11-12 [redacted] SAC & Program Manager Conf Flag, Rm. HQ	31 [redacted] SAC & Program Manager Conf Flag, Rm. HQ			

b6
b7C
b7E

b6
b7C
b7E

2007

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

February

Sun	Mon	Tue	Wed	Thu	Fri	Sat
				1 [redacted] 10-11 [redacted] 4	2 10-11 [redacted] 4	3
4	5 CI Espionage Course [redacted] QT	6 CI Espionage Course	7 [redacted] CI Espionage Course	8 [redacted] a CI Espionage Course	9 CI Espionage Course	10
11	12 CIOPS 0702 QT	13 CIOPS 0702 SAC & Program Manager Conf [redacted]	14 CIOPS 0702 SAC & Program Manager Conf	15 CIOPS 0702	16 CIOPS 0702	17
18	19 Holiday CIOPS 0702	20 CIOPS 0702	21 CIOPS 0702	22 CIOPS 0702	23 CIOPS 0702	24
25	26 CIOPS 0702	27 [redacted] FBI and Federal Partners [redacted] CIOPS 0702	28 CIOPS 0702			

2007

b6 b7C b7E

b6 b7C b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

March

Sun	*Mon*	*Tue*	*Wed*	*Thu*	*Fri*	*Sat*
				1 CIOPS 0702 CP Practical (TBA) [redacted]	2 CIOPS 0702	3
4	5 [redacted] 3:30 - 4:45pm CIOPS 0702	6 [redacted] CIOPS 0702	7 CIOPS 0702	8 CIOPS 0702	9 CIOPS 0702	10
11	12 CIOPS 0703 QT	13 [redacted] FBI and Federal Partners CIOPS 0703	14 CIOPS 0703	15 CIOPS 0703	16 CIOPS 0703	17
18	19 CIOPS 0703	20 CIOPS 0703	21 CIOPS 0703	22 CIOPS 0703	23 CIOPS 0703	24
25	26 CIOPS 0703	27 CIOPS 0703	28 CIOPS 0703	29 CIOPS 0703	30 CIOPS 0703	31

b6
b7C
b6
b7C
b7E
b6
b7C
b7E

2007

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

April

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2 3:300-4:45 [redacted] CIOPS 0703	3 [redacted] CIOPS 0703	4 CIOPS 0703	5 CIOPS 0703	6 CIOPS 0703	7
8 EASTER	9	10 [redacted] [redacted]urse 0702 QT [redacted]	11 FTS 10-11 [redacted] CP[redacted]	12 FTS 10-11 [redacted] CP[redacted]	13 FTS 10-11 [redacted] CP[redacted]	14
15	16 CI[redacted]Course 0702 QT [redacted]	17 CI[redacted] Course 0702	18 CI[redacted] Course 0702	19 CI[redacted] Course 0702 [redacted] 11-12 [redacted]	20 CI[redacted] Course 0702	21
22	23 CP Overivew/Tools for IAs location Spy Museum (funding pending) [redacted] CI[redacted]Operations Course QT 0702 Lum	24 CP Tools CI[redacted]Operations Course 0702	25 CP Tools CI[redacted]Operations Course 0702	26 CP Tools CI[redacted]Operations Course 0702	27 CP Tools CI[redacted]Operations Course 0702	28
29	30 CIOPS 0704 QT					

2007

b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

May

Sun	Mon	Tue	Wed	Thu	Fri	Sat
		1 CIOPS 0704	2 CIOPS 0704	3 CIOPS 0704	4 CIOPS 0704	5
6	7 CIOPS 0704	8 ICOC 11-12 [redacted] CIOPS 0704	9 CIOPS 0704	10 CIOPS 0704	11 CIOPS 0704	12
13 Mother's Day	14 CIOPS 0704	15 CIOPS 0704	16 CIOPS 0704	17 CIOPS 0704	18 CIOPS 0704	19
20	21 CIOPS 0704	22 CIOPS 0704	23 CIOPS 0704	24 CIOPS 0704	25 CIOPS 0704	26
27	28 Holiday	29	30	31		

2007

b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

June

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					1	2
3	4 CIOPS 0705 QT	5 time TBA FBI and Federal Partners [redacted] CIOPS 0705	6 CIOPS 0705	7 CIOPS 0705	8 CIOPS 0705	9
10	11 CIOPS 0705	12 ICOC 11-12 [redacted] CIOPS 0705	13 CIOPS 0705	14 CIOPS 0705	15 CIOPS 0705	16
17 Father's Day	18 CIOPS 0705	19 CIOPS 0705	20 CIOPS 0705	21 CIOPS 0705	22 CIOPS 0705	23
24	25 CIOPS 0705	26 CIOPS 0705	27 CIOPS 0705	28 CIOPS 0705	29 CIOPS 0705	30

2007

b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

July

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4 Holiday	5	6	7
8	9 CIOPS 0706 QT	10 CIOPS 0706	11 CIOPS 0706	12 CIOPS 0706	13 CIOPS 0706	14
15	16 CIOPS 0706	17 ICOC 11-12 [redacted] CIOPS 0706	18 CIOPS 0706	19 CIOPS 0706	20 CIOPS 0706	21
22	23 CIOPS 0706	24 CP Seminar [redacted] CIOPS 0706	25 CP Seminar CIOPS 0706	26 CP Seminar CIOPS 0706	27 CIOPS 0706	28
29	30 CIOPS 0706	31 CIOPS 0706				

b6
b7C
b7E

b6
b7C
b7E

2007

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/EAW/STP/bls

August

Sun	Mon	Tue	Wed	Thu	Fri	Sat
			1 CIOPS 0706	2 CIOPS 0706	3 CIOPS 0706	4
5	6 CI [redacted] Course 0703 QT [redacted]	7 CI [redacted] Course 0703	8 CI [redacted] Course 0703	9 CI [redacted] Course 0703	10 C [redacted] Course 0703	11
12	13 CI for Intelligence Analysts 0701 QT	14 CI for Intelligence Analysts 0701	15 CI for Intelligence Analysts 0701	16 CI for Intelligence Analysts 0701	17 CI for Intelligence Analysts 0701	18
19	20 Managing CI Investigations and Operations 0702 QT	21 ICOC 11-12 [redacted] [redacted] Managing CI Investigations and Operations 0702	22 Managing CI Investigations and Operations 0702	23 Managing CI Investigations and Operations 0702	24 Managing CI Investigations and Operations 0702	25
26	27 CI [redacted] Operations Course 0703 QT [redacted]	28 CI [redacted] Operations Course 0703	29 CI [redacted] Operations Course 0703	30 CI [redacted] Operations Course 0703	31 CI [redacted] Operations Course 0703	

b6 b7C b7E

b6 b7C b7E

b6 b7C b7E

2007

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

September

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3 Holiday	4	5	6	7	8
9	10 CI for Intelligence Analysts Course 0702 QT	11 CI for Intelligence Analysts Course 0702	12 CI for Intelligence Analysts Course 0702	13 CI for Intelligence Analysts Course 0702	14 CI for Intelligence Analysts Course 0702	15
16	17 CI Humint Operations Course 0704 QT [redacted]	18 CI Humint Operations Course 0704	19 CI Humint Operations Course 0704	20 CI Humint Operations Course 0704	CI Humint Operations Course 0704	22
23	24 CIOPS 07-07	25 ICOC 11-12 [redacted] CIOPS 07-07	26 CIOPS 07-07	27 CIOPS 07-07	28 CIOPS 07-07	29
30						

2007

b6
b7C

b6
b7C
b7E

DATE: 01-11-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-11-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Joint Counterintelligence Training FBI [redacted]

(S) b1 b7E

(S) **1. Cross-agency training (FBI [redacted])?**

(S) CITC offers training in, and or conducts, the following training [redacted]:

1) Slots in the CITC's Counterintelligence Investigations and Operations Course (four week intermediate CI training)

2) Executive Manager's Course

3) FBIHQ Unit specific conferences

(S) 4) Blocks of instruction in [redacted] Hostile Environment Training Course

(S) 5) Blocks of instruction in [redacted] New Officer Training

6) Two CD-ROM interactive interview simulation courses

(S) [redacted] b1 b7E

~~SECRET~~

2) Training prior to 9/11/01?

CI cross training prior to 09/11/01 consisted of FBI Unit specific conferences and Integrated Field Operation (surveillance) courses.

3) Training after 9/11/01?

CI training after 9/11/01 is as listed in #1 above.

4) Number of people involved in such training?

Unclear whether this means people instructing the training, receiving the training, or what period they are interested in.

5) Nature of training before/after 9/11/01?

See numbers #1 and #2 above.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-11-2012 BY 65179/DMH/BAW/STP/bls

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 12/3/2008

To: All Divisions **Attn:** Chief Division Counsel
Human Source Coordinators

From: Directorate of Intelligence

Office of the General Counsel
Investigative Law Unit
Contact: [redacted]

Approved By: Favreau Kevin
Caproni Valerie E
Lammert Elaine N
Thomas Julie F
[redacted]

b6
b7C
b7A
b7E

Drafted By: [redacted] :blm

Case ID #: [redacted] (Pending)

Title: INVESTIGATIVE MATTERS;
LEGAL GUIDANCE: INTERIM LEGAL GUIDANCE REGARDING USING AN ASSESSMENT UNDER THE NEW ATTORNEY GENERAL GUIDELINES TO IDENTIFY, ASSESS, VALIDATE OR MAINTAIN THE COVER OR CREDIBILITY OF A CONFIDENTIAL HUMAN SOURCE

Synopsis: To provide interim legal guidance regarding techniques which may be utilized for the assessment of Confidential Human Sources (CHSs) under the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM) pending development of policy by the Directorate of Intelligence (DI).

Details: (U) On November 26, 2008, the Attorney General signed an order providing, in substance, that any lawful technique, not just "assessment techniques," can be used by the FBI to identify potential human sources and assess their suitability or credibility. In anticipation of this added flexibility, the AGG-DOM and the Domestic Investigations and Operations Guide ("DIOG") provide the flexibility to utilize techniques to vet or validate a source that are not permissible in other types of assessments. Because it is prudent to ensure that the techniques and approval levels contained in the Confidential Human Source Manuals complement and are consistent from a policy perspective with the

To: All Divisions From: Office of the General Counsel
Re: [redacted] 12/3/2008

b7A
b7E

approach taken in the DIOG, until further policy is issued, the techniques authorized to identify, assess, validate or maintain the cover or credibility of a source are limited to those techniques identified specifically in Section II.A(4) of the AGG-DOM. Because the vetting and validating of a source are not appropriate subjects for a grand jury investigation, although grand jury subpoenas for subscriber information may be issued in certain types of assessments, they cannot be used for this purpose. Thus, until you receive further guidance from OGC and the DI, only the following techniques may be used to identify, assess, validate or maintain the cover or credibility of a source:

1. obtaining publicly available info;
2. accessing and examining FBI and DOJ records;
3. accessing and examining records maintained by, and requesting information from, other federal, state, local, tribal or foreign government entities or agencies;
4. using online services and resources (whether nonprofit or commercial);
5. interviewing or requesting information from members of the public and private entities;
6. accepting information voluntarily provided by governmental or private entities; and
7. engaging in observation or surveillance not requiring a court order.

To: All Divisions From: Office of the General Counsel
Re: [redacted] 12/3/2008 b7A

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

For dissemination by Chief Division Counsels to all appropriate Field Office personnel including all Confidential Human Source Coordinators.

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

CIOPS/IMIS COURSES
Topical Comparison

CIOPS	IMIS
Fundamentals of FBI-CI	Fundamentals of FBI CI
• Definition of CI	• Definition of CI
• 3 Primary CI Objectives	• 3 Primary CI Objectives
• Key Historical Events	• 5 CI Program Goals
• Basic Concepts (Proactive)	•
•	•
o	
o	
o	
	Differences between Criminal and FCI Cases/Terminology
The Adversary	
•	
• mission	
Classification and Security Issues	Classification and Handling Classified Information
• How to classify and mark	• How to mark
• Standard Identification Markings	• Standard Identification Markings
• Transporting/routing classified information	• Transporting/routing classified information
•	• Copying classified information
• Storing classified information	• Storing classified information
• Safeguarding classified information	• Safeguarding classified information
A History of FCI Authority	
• Non-statutory authority (EOs, etc.) Overview	
• Statutory authority Overview	
• The USIC (review)—Role in the IC	USIC Members and their Role in the IC
• The National Security List Overview	NSLs—definition
o Country Threats	• Country Threats
o Issue Threats	• Issue Threats
Report Writing & Dissemination	
FBI Asset Administration Issues	FBI Assets
• Source	• Source
• Asset	• Asset
• Asset	• Asset
•	• Summary of
	• PI on an Asset
	o Asset background investigation

b7E

b6
b7C
b7E

b7E

~~SECRET~~

b1
b6
b7C
b7E

CIOPS	IMIS
	o Minimum investigative techniques to use
	o Initial asset interview
	o [redacted]
[redacted]	
• Reporting requirements	• Asset Reporting
[redacted]	
• Administrative issues	• Administrative Issues
o Asset payments/assoc. expenses	o Asset payments/assoc. expenses
o Asset case funding	o Asset case funding
o Closing an asset	o Closing an asset
FCI Authority [redacted]	FCI Authority (Overview)
• Statutes	• Title 18 (Sections 1831 and 1832)
o Title 50	• Title 50
• EO 12333	• EO 12333
• FISA	• FISA
• EEA of 1996	• Economic Espionage Act of 1996
• NSIG	• FCI AGG
o Threat Assessment Activities	o Threat Assessment Activities
o PIs	o PIs
• predications for	• predications for
• investigative techniques	• investigative techniques
o FIs	o FIs
• predications for	• predications for
• investigative techniques	• investigative techniques
o Converting a PI to a Full	o Converting a PI to a Full
	o Case Resolution/Closing
CI Resources	
The [redacted] —Purpose	Recruitment—Purpose
• Reasons for knowing [redacted]	•
• [redacted]	• [redacted] b7E
	o
The FCI [redacted] Technique	FCI [redacted]
• Types	• Types
• Subjects	• Subjects b7E
• Primary objective	• Primary objective
• [redacted]	• [redacted]
• Interviews [redacted]	• Interviews [redacted] pproach)
FCI Interviews/Interrogations	FCI Subject Interviews
• Subject interviews	

ACLURM032264

CIOPS	IMIS
Analysis	
Positive Intelligence Reporting (IIRs)	
Cultural Considerations	
• [redacted]	
•	
•	
[redacted] Fundamentals	
[redacted]	
• Admin requirements	
• Environmental requirements	
• Human Factors	
• Technical issues	
• [redacted] concepts	
• Foot-based [redacted]	
• Vehicle-based [redacted]	
Surveillance Photography	
Surveillance Planning and Execution	Surveillance [redacted]
[redacted]	
	• ELSUR vs. Physical Surveillance [redacted]
	• [redacted]
	• [redacted]
SSG Capabilities	
Counterproliferation	
Undercover Operations	
Behavioral Analysis Program	Behavioral Analysis Program (defined)
[redacted]	[redacted]
	• [redacted]
FISA	FISA
• History	• History (Church Committee)
• Statute/Minimization	• FISC
• Drafting Application	• FISA Application Process
•	• As an Investigative Tool

(S) (S) (S) (S) (S)

b7E b1 b7E b1 b7E b1 b7E

ACLURM032265

b1
b7E

CIOPS	IMIS
•	
Using GPS	
Economic Espionage - Working with the Business Community	Economic Espionage Act of 1996
Espionage Investigations	Espionage Investigations
	• Defined
	• Principle Statutes
	o Title 18 (defined and quoted)
	o Title 50 (defined and quoted)
	o Comparison of Titles 18 and 50
	o Intelligence Authorization Act of 1990
	o EO 12333
	• Counterespionage Section at DOJ
Implementing the National CI Strategy in the Field	
	Caseload Management/Prioritization (investigative association)
	• Minimum FCI investigative efforts required
	• FCI case administrative requirements

CIOPS Case Presentations	IMIS Case Presentations
(SSG)	Ronald William Pelton (Espionage)
Hanssen (Espionage)	Christopher M. Cooke (Espionage)
George Trofimoff (Espionage/Reactivation	Thomas Patrick Cavanagh
John Walker (Espionage)	Dimitri Fedorovich Polyakov
	Colonel Oleg Penkovsky
	Ana Belan Montes (Espionage)
	George Trofimoff (Espionage and Surveillance)

b1
b6
b7C
b7E

	Kim Philby (DA)
	Randy Miles Jefferies (Espionage)
	Kurt G. Lessenthien (Espionage)

Topics/Lessons Covered in CIOPS but not in IMIS

Briefings

- [redacted]

USIC Briefings

(S) [redacted] b1 b7E

- Dinner meeting (optional)

Section Briefings

- CD-1
  - [redacted]
- CD-2
  - [redacted] b7E
- CD-3
  - [redacted]
- CD-4
  - [redacted]

Practicals

(S)
- "Break the Ice" Practical Exercise (Role Players)
  questions and problems
(S)
- Rotating Interview Problems (Role Players)
- Demonstrations
(S)

b1
b7E

Topics/Lessons Covered in CIOPS but not in IMIS

Cuban Missile Crisis Narrative
Surveillance of Pitts
(S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

Basic CI Operations

Topical Areas to Cover

- How cases typically begin

(S) [redacted] b1 b7E

- LHMs
  - Who to write to
  - What to write for
  - Timelines for writing

- Definitions

(S) [redacted] b1 b7E

- Techniques to use when working a CI case

(S) [redacted]

~~SECRET~~

ACLURM032269

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

Meeting with CD Assistant Section Chiefs
Feedback/Recommendations Regarding CIOPS

June 16, 2005

Attendees:

[redacted] b6 b7C

General Comments

[redacted] on subjects—teach thoroughness across programs. b7E

Techniques vs. [redacted] –get best practices from SC's in CD.

Goals/stats are NOT global in nature. Prosecution??

[redacted] b7E

[redacted] b7E

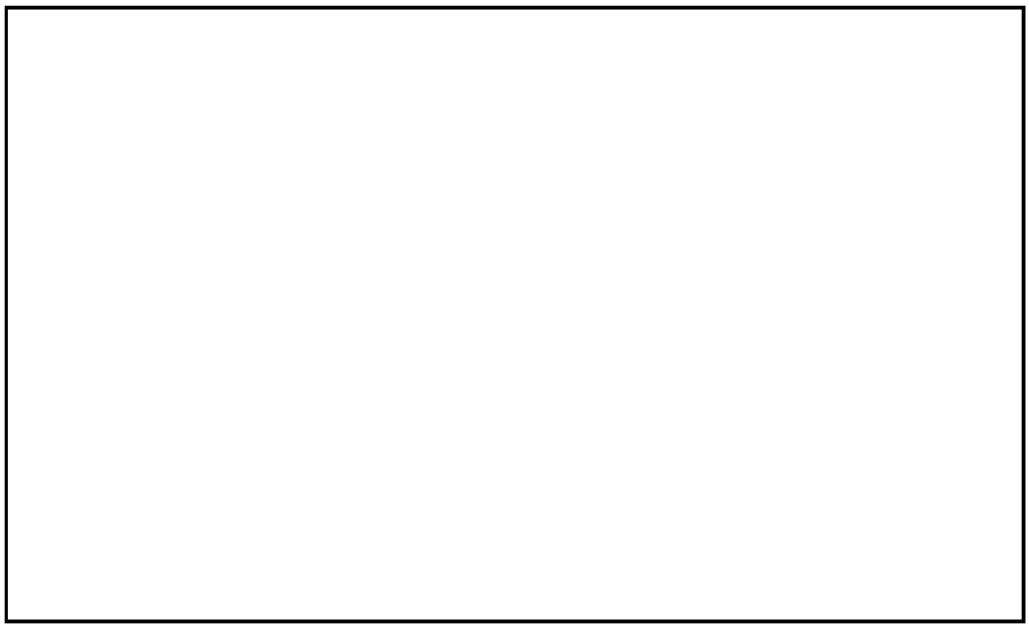
Country and culture information. Set a homework assignment BEFORE reaching class to find and give information on where on the Intranet they can find information.

Key concepts to focus on:

[redacted] b7E

Movement/Analysis

Agents should do movement analysis and other analyses as part of their basic homework. They can use MS Access or other programs to produce a timeline of sorts, as well as a database in which to hold all kinds of information (combine surveillance logs with telephone tolls, etc.).



b7E

Country/Culture

Introduce them to the *CIA World Factbook* on the Intranet.

Paperwork

Need to work on documentation!!! They use too much passive voice, "the Source said…"

They need to know how to write intelligence debriefs. Need clear, complete ECs. We're getting piecemeal information—no logical follow-up (who, what, when, where, why, how questions answered) based on responses to initial questions. For example, how did the source get the information? What kind of subsourcing has occurred?

Must be done by example. Get it on paper and to HQ.

IIRs—there's a rush to put stuff out to the community, but we've got NO FOLLOW THROUGH. (They ask the first question, but don't go beyond it.) Then the community has a whole lot of questions.

Our Agents are submitting drafts as final products.

Raw report doesn't mean necessarily that you can't use your judgment. Use the assets to produce intelligence. Think like an IO when dealing with the asset/source.

b7E

What is the Agents job? FBI jurisdiction. WE put out the information NOT [redacted]

PAPERWORK: LHMs and be VERY poor. Agents are giving no thought to source protection when writing their LHMs. Get examples of this. Include in the training what other agents DO and DON'T need to know. What's admin data vs. important info. They must figure out what information is important ONLY to the FBI and leave that OUT of the LHMs.

They need to stop putting in so much unnecessary detail. They are BURYING the important information in the body of their documentation.

Assets

IIRs—there's a rush to put stuff out to the community, but we've got NO FOLLOW THROUGH. (They ask the first question, but don't go beyond it.) Then the community has a whole lot of questions.

Assets—a lot of damage can be done with the IIRs—we can lose our credibility. For example, we cannot simply take for granted everything our assets say.

The Agents are shooting stuff to Pistole or Director Mueller, past the CD Operational Divisions, as urgent reports—but a lot of the stuff IS NOT credible. Our assets CAN and DO misfeed information to us (perhaps not even knowingly—they may be getting their information from too many subsources).

b7E

We need to focus on [redacted] *information, not just any information.*

[redacted]

b7E

In class: Debrief a source and have them deal with it. How to write it up.

[redacted]

b7E

ALWAYS be skeptical with source information.

Liaison/Working with Other Agencies

The days of our keeping the information to ourselves are gone. The ASAC and SSAs still have a no-share attitude. We MUST get rid of this. We need to look at information and try to get not only what we want, but [redacted] b7E

[redacted]

Please call HQ FIRST before sharing information OR taking leads based on gaps from others in the IC community (i.e., commerce, customs, NR or their area desks). Always coordinate with HQ FIRST!

Learn the roles of the NR and their area desks.

Have [redacted] explain how NR operates vs. the CI Center vs. the country desks. They ARE different from each other. b6 b7C

NR is an INTERFACE only (not the authority) between the FBI and [redacted]

The students MUST read the MOU with [redacted]. b7E

SIT DOWN with your [redacted]. Make it clear that ALL they do MUST be coordinated through the FBI. The need to SHARE in the production of this. If you are not careful, you'll lose operational control to [redacted]. Ask HQ FIRST BEFORE running joint [redacted]

Jurisdiction and export violations. [redacted] gives a good presentation on this. Deputy to [redacted]—FBI rep. from Customs. Add what's common in this among all the programs. All the different agencies/entities spend A LOT of time in liaison. b7E

Changed laws—NSA, Commerce, State, Customs—need a consensus of all on their roles.

On joint investigations—the investigation currently tends to consist of reporting what the other agency is doing instead of investigating things themselves. They are seeming overwhelmed and/or lazy based on the streamlining HQ is seeing. (They give status reports saying the same thing time after time.)

Coordination with HQ Substantive Units

Get country and culture information—put into page-long laminated "cheat sheets."

Casework

(S) 1. [redacted] b1 b7E

(S) [redacted] b1 b7E

2. (S) [redacted]

3. [redacted]

4. **Espionage** (S) [redacted] They need to start using BASIC INVESTIGATIVE techniques EVERY time they open a [redacted] case. DON'T take shortcuts and go right to a sophisticated operation. They MUST prepare for it.

(S) [redacted] b1 b7E

5. (S) [redacted]

Supervisor Course:

(S) SSA [redacted] supervisor course vs [redacted] supervisor course. b1 b7E

(S) SSAs need Espionage [redacted] and [redacted] training.

Assistant Section Chief Taskings:

1. ID cases to review ([redacted] not necessarily use. b6 b7C b7E
2. get examples/samples of good & bad writing
3. give best practices on [redacted]

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-12-2012 BY 65179/DMH/BAW/STP/bls

New Agents Instructional Objectives for Intelligence Investigative Training Unit (ITU), TDD

General ITU

1. List the core capabilities of the FBI to include investigative, intelligence, strategic partnerships, investigative technologies, and forensic capabilities.
2. List and describe six databases commonly used in FBI investigations;
3. Explain how to access the databases described above;
4. Describe the information that can be obtained from each database.
5. Describe, in general terms, how an FBI investigation is opened;
6. Recognize and differentiate between the various parts of an FBI file number;
7. Define the meaning of FBI "serials" and "sub-files."
8. List and describe at least six investigative techniques used in FBI investigations;
9. Explain the "least-to-most intrusive" approach to the use of investigative techniques in FBI investigations;
10. Describe the three levels of investigative activity as set forth in the AGG for General Crimes and identify which investigative techniques can be used at each level;
11. Recognize three differences between Criminal and National Security investigations as it relates to the use of investigative techniques.
12. Define the meaning of [redacted] investigations; b7E
13. Working from least to most intrusive, select appropriate investigative techniques to apply in reactive investigations (specifically fugitive and bank robbery investigations).
14. Define domestic terrorism and differentiate between domestic and international terrorism;
15. Define and describe four domestic terrorism organizations currently operating in the United States;
16. Differentiate between left-wing, right-wing, and other domestic terrorism organizations;
17. Working from least to most intrusive, select appropriate investigative techniques and apply those techniques to a domestic terrorism fact situation;
18. List and describe the three-part process for telephone information gathering;
19. Differentiate between the functions of pen registers and trap and traces;
20. Describe how to conduct a [redacted]
21. List and discuss [redacted]
22. Describe an investigative plan appropriate for the new fact pattern.
23. Define the terms "White Collar Crime," "Fraud," and "Criminal Intent."
24. List and describe the investigative techniques commonly used in financial crimes investigations; and
25. Describe the [redacted] and explain its applicability to financial crimes investigations. b7E
26. Describe the role of the Federal Grand Jury in criminal investigations;
27. Differentiate between Administrative Subpoenas and Grand Jury Subpoenas;
28. List five Title 18 statutes used in financial crimes investigations and outline the elements necessary to prove these violations.
29. Recognize common schemes and be able to select and apply the appropriate investigative techniques, working from least to most intrusive, for each type of fraud scheme;
30. Compare which investigative techniques generate the best evidence in a fact situation.
31. At the end of this two-hour block of instruction, students should be able to:
32. Define asset forfeiture and differentiate between civil and criminal forfeiture;
33. Define money laundering and identify two Title 18 statutes applicable to money laundering violations;
34. Outline the elements necessary to prove the two money laundering statutes;
35. At the end of this four-hour block of instruction, students should be able to:

ACLURM032275

36. Appreciate the importance and necessity of contributing to the FBI's intelligence base;
37. Define and differentiate between confidential informants, cooperative witnesses, and assets.
38. Distinguish categories and classifications of sources, including alpha designations, substantive file numbers, code names and symbol numbers.
39. Discuss the [redacted] and identify potential pitfalls within each step of the [redacted]
40. Describe the common motivations of sources in FBI investigations and their role in source development and use;
41. Identify [redacted]
42. Differentiate between the source Main File and Sub A file;
43. Define and describe the [redacted] period for Confidential Informants; b7E
44. Define and describe source "admonishments;"
45. Define "Otherwise Illegal Activity (OIA)" and distinguish between Tier 1 and Tier 2 OIA.
46. By the end of this two-hour block of instruction, students should be able to:
47. List [redacted] in FBI investigations;
48. Explain the steps necessary to have [redacted]
49. Describe what it means to [redacted]
50. Explain the approval process necessary to [redacted]
51. Explain what approval authority is necessary to [redacted]
52. Define what constitutes an undercover operation;
53. Differentiate between [redacted]
54. List and define five UCO sensitive circumstances;
    a. Relate the basic legal and administrative requirements of a Title III;
    b. Determine whether a specific criminal violation is a Title III predicate offense for wire or oral interceptions;
    c. Conduct the three-pronged analysis regarding core of Title III affidavit;
55. Define the concept of "enterprise theory of investigation" and describe how it is applied to FBI investigations;
56. List three statutes often used to prosecute criminal enterprises;
57. Define the concept of "criminal intelligence investigations" and distinguish between REIs and TEIs;
58. Describe administrative steps to open a cooperative witness;
59. List and describe steps necessary to conduct consensual monitoring.
60. By the end of this two-hour block of instruction, students should be able to:
61 Demonstrate a strategy of how to apply investigative techniques to a fact situation, using the "least-to-most" intrusive approach;
62. Prepare a summary of the elements of a specific financial crimes-related statute and explain what investigative techniques would be appropriate for proving a violation of that statute;
63. By the end of this two-hour block of instruction, students should be able to:
64. Describe how to open an individual as a confidential informant;
65. Describe the necessary steps/process when an open source engages in unauthorized criminal activity;
66. By the end of this two-hour block of instruction, students should be able to:
67. Discuss how to get authority to use various sophisticated investigative techniques, such as undercover operations and Title III wiretaps.
68. List steps necessary to make controlled drug purchase.
69. Distinguish between types of existing law enforcement partnerships and legal underpinnings for those partnerships.
70. Appreciate the importance of liaison to the FBI's ability to serve the American public.
71. Define consensual monitoring and distinguish it from non-consensual monitoring;
72. Describe the approval authorities and paperwork necessary to properly engage in consensual monitoring;

73. Appreciate the importance that electronic surveillance has to an investigation, particularly as it applies plea negotiations and to a jury.

Case Management

1. Describe, in general terms, the structure and organization of the FBI;
2. Define the role of the Special Agent in federal investigations and differentiate this role from that of the AUSA;
3. List and briefly describe the four phases of an investigation.

Intelligence Requirements

1. Define the meaning of intelligence requirements;
2. Discuss how intelligence requirements are formulated;
3. List the steps necessary to locate appropriate intelligence requirements for whatever investigative matter is being worked.

ACLURM032277

FBI031797

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

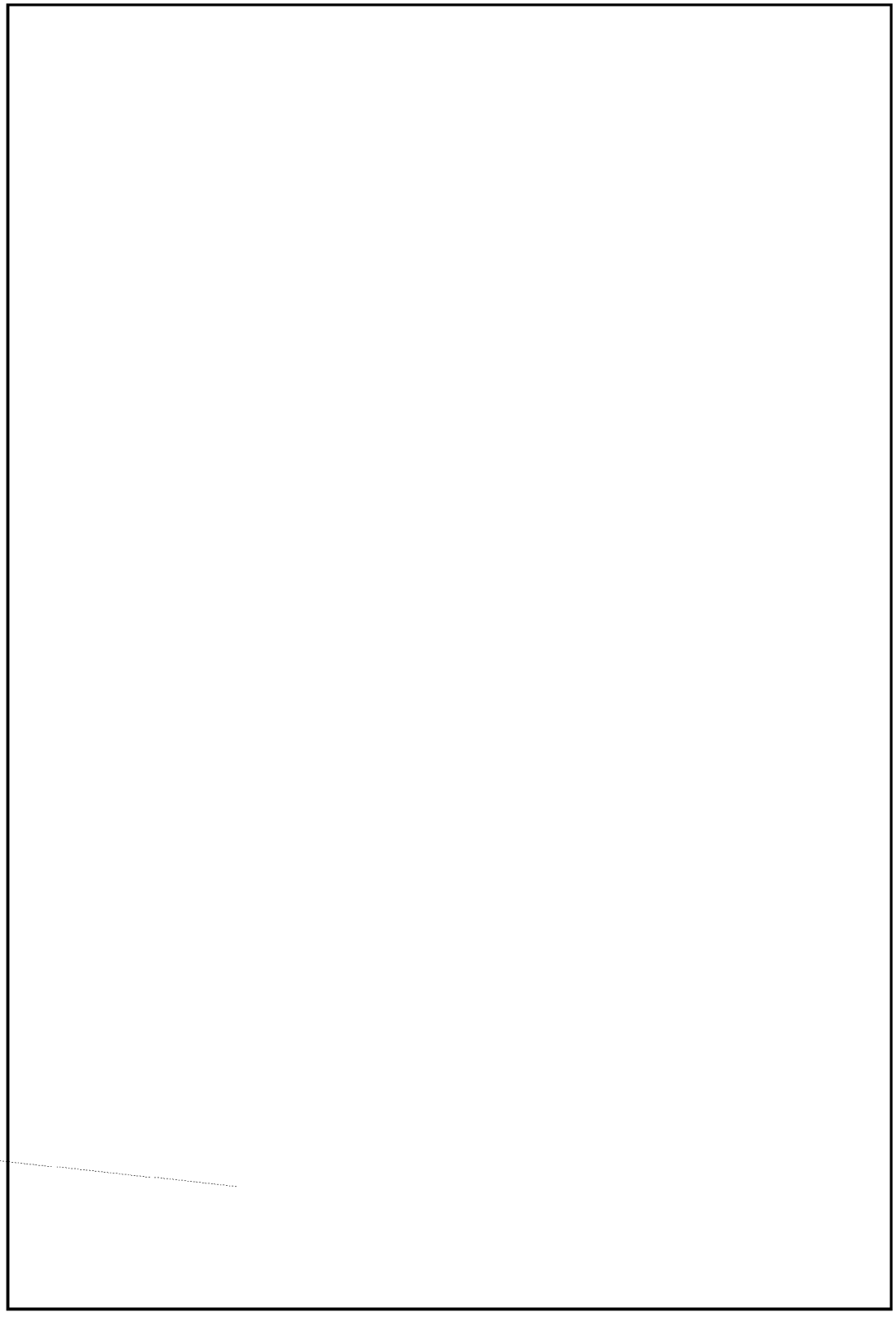
DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

CIOPS IOs Based on [ ] Write-up

b6
b7C

b1
b7E

(S)



~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-12-2012 BY 65179/DMH/BAW/STP/bls

09/13/06

Counterintelligence Program for New Agents

Course Goals- This course addresses the key aspects of Counterintelligence (CI) threat, strategy and operations. Students will obtain a brief history of CI, a basic understanding of the objectives of CI, and the role of CI and criminal agents in meeting those objectives. The instructional design of the training will include lecture, tests and practical problems.

Instructional Objectives -

Day #1

Introduction to CI - A History - Upon completion the student will be able to identify critical events in CI history, and the goals and objectives of the CI program. The student will be able to recognize, identify, and explain various methods of [redacted] b7E

Day #2

[redacted] b7E

Day #3

[redacted] b7E

Day #4

[redacted] b7E

ACLURM032279
FBI031799

Day #5



b7E

ACLURM032280

FBI031800

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-17-2012 BY 65179/DMH/BAW/STP/bls

+ **AM [redacted] Demonstration Exercises** b7E

Role players should be in place by no later than 8:45AM. Kick-off will begin at **9:00**, role players are expected to speak to each of the 4 groups for twenty minutes. At **9:40** students will break for 20 minutes and at **10:00** will be in place for last 2 demonstrations. Role players should inform, engage and encourage student participation. At the end of **all** demonstrations, prior to lunch students will gather on the south side of [redacted] for briefing regarding afternoon practical. Students are not to use radios for AM practical. Punctual from breaks.

Role players AM	Name	Name	Observer
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
SRAC role player	[redacted]		

b6
b7C

Instructors: [redacted] b6 b7C

ACLURM032281

Role players should be in place for PM exercise by no later than 12:00.

IO and monitor reminders:
Monitors should be in place no later than **12:00** to meet their teams at designated spots and **promptly begin** demonstration at **12:15**. Monitors will **contact** [redacted] @ [redacted] to indicate the kick-off of demonstration and at the end of first demonstration.

b6
b7C
b7E

IOs can place students out of play if too aggressive. Starting point is ending point. At conclusion have students gather as a team and note on 3X5 card how many operational acts they observed. Include on 3X5 location, type and any descriptive data noted. IOs and monitors should walk through SDR with students for final review and comments. (Please ensure students are familiar with terms such as: [redacted] Please release students **no later than 3:30pm. At the end of day please return all** [redacted] **to CITC instructors**.

Student reminders:
Students are working as SAs of WFO during PM exercise. WFO surveils [redacted] does not [redacted] but proceeds to [redacted] Surveillance reports that [redacted] engaged in apparent op activity in [redacted] and observes what appears to be a [redacted] between IO and UNSUB in vehicle with VA tags. Tags traced to [redacted]

b6
b7C
b7E

Students should look for [redacted] All vans parked [redacted] parking lot.

ACLURM032282
FBI031802

PM Locations	Intelligence Officer	Monitor
Library -		
Visitor Center		
		(Parking Lot)
		Need tag#
At least three not seen by students, SRAC can change jacket.		

b6
b7C
b7E

b6
b7C
b7E

ACLURM032283

Counterintelligence Surveillance Course 08-01 Agenda

	Classroom	Conference Room	Room 310	Room 410	
	[redacted]	[redacted]	[redacted]	[redacted]	b6 b7C
8:00-8:50	Introduction, Administration, & Course Information Classroom				
9:00-10:30	Group 1 CI Objectives: [redacted]	Group 2 [redacted]	Group 3 Introduction to [redacted] Fundamentals of [redacted] Operational Activities: [redacted] Acts, Configuration, Environment, and Flow	Group 4 [redacted]	b1 b7E
10:45-12:15	Group 4 CI Objectives: [redacted]	Group 1 [redacted]	Group 2 Introduction to [redacted] Fundamentals of [redacted] Operational Activities: [redacted] Acts, Configuration, Environment, and Flow	Group 3 [redacted]	b1 b7E
12:15-1:15	LUNCH				
1:15-2:45	Group 3 CI Objectives: [redacted]	Group 4 [redacted]	Group 1 Introduction to [redacted], Fundamentals of [redacted] Operational Activities: [redacted] Acts, Configuration, Environment, and Flow	Group 2 [redacted]	b1 b7E
3:00-4:30	Group 2 CI Objectives: [redacted]	Group 3 [redacted]	Group 4 Introduction to [redacted], Fundamentals of [redacted] Operational Activities: [redacted] Acts, Configuration, Environment, and Flow	Group 1 [redacted]	b1 b7E
4:45-5:30	Discussion & Review in Classroom				

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

COUNTERINTELLIGENCE SURVEILLANCE COURSE #08-01

August 25, 2008:

0800 - 8:50 Introduction, Administration, and Course Information

0900 - 10:30 Counterintelligence Objectives:

(S) [redacted] b1 b7E

10:45 - 12:15

(S) [redacted]

12:15 - 1:15 Lunch

1:15 - 2:45 Introduction to [redacted] Fundamentals of

(S) Operational Activities [redacted] b1 b7E

3:00 - 4:30

(S) [redacted]

4:45 - 5:30 Discussion and Review in Classroom

5:30 Break

(S) **August 26, 2008:**

0800 - 8:50 [redacted]

(S) 9:00 - 12:00 Introduction [redacted]

(S) a. [redacted]
b.
c.
d.
e.
f.
g.

b1
b7E

12:00 - 1:00 Lunch

1:00 Surveillance Practical Problem

5:00 Conclude Surveillance Practical Problem

August 27, 2008:

0800 - 11:30 Surveillance Practical and [redacted] Demonstrations b7E

12:30 - 1:30 Lunch (Box lunches from Academy Available upon request)

1:30 - 5:00 Continuation of Surveillance Practical and [redacted] Demonstrations

August 28, 2008:

(S) 0800 - 10:00 [redacted] b1 b7E

(S) 10:00 - 12:00 Advanced [redacted]

12:00 - 1:00 Lunch

1:00 Surveillance Practical Problem

5:00 Conclude Surveillance Practical Problem

August 29, 2008:

0800 Instructions for Phase II:
- Rules of Engagement
- Boundaries
- Expectations
- Logistics

1000 [redacted] familiarization

b7E

August 30 - September 5, 2008:

0700 Command Post Opens

2330 Command Post Closes

September 5, 2008:

1000 Dismissal

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 01-12-2012
CLASSIFIED BY 65179/DMH/BAW/STP/bls
REASON: 1.4 (c)
DECLASSIFY ON: 01-12-2037

7/15/2011

(S)

DEFINITIONS

b1
b7E

WHO UTILIZES

(S)

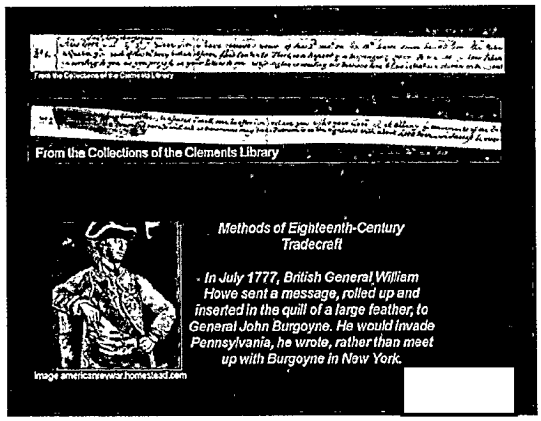
(S)

TYPES OF

b1
b7E

Cryptology/Cryptography or Secret Writing

The term "cryptography" ("secret writing," from the Greek *kryptós*, "hidden," and *gráphein*, "to write") is often used to refer to the field as a whole, as is "cryptology" ("the study of secret writing").



b1
b7E



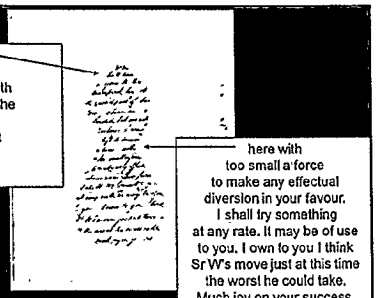
A simple method of secret writing that the Americans never caught on to:

An apparently unexceptional letter from General Henry Clinton contained a secret message hidden in plain sight.



When a mask, usually posted by separate mailing, was placed over the letter, the self-contained section with the covert message was revealed.

b7E



The intended message, in which not being able to persuade Howe to move up to New York instead of Pennsylvania: "Sr W's move just at this time / the worst he could take."

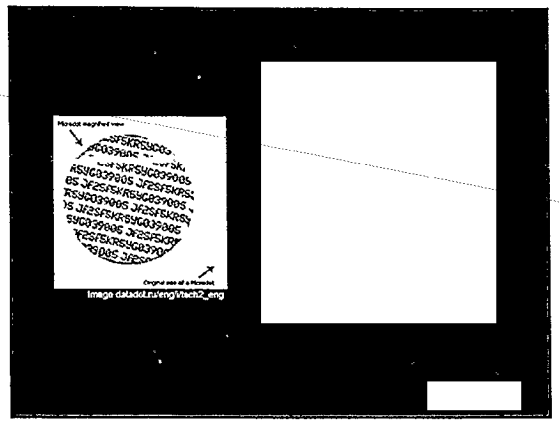


b7E

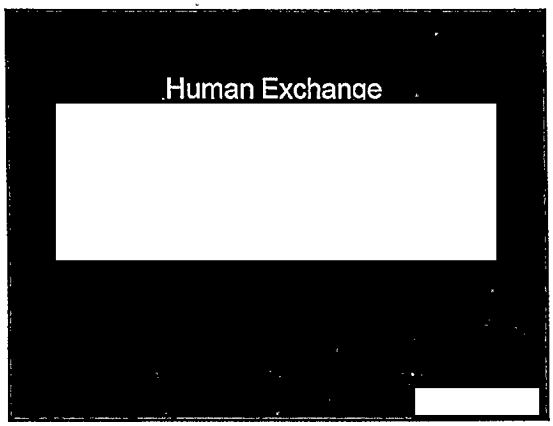


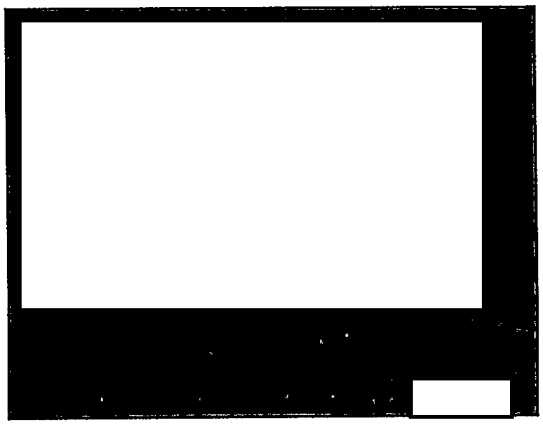
b7E

(S)



b1
b7E

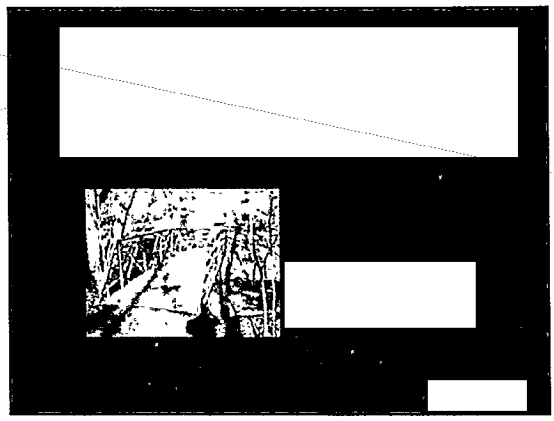


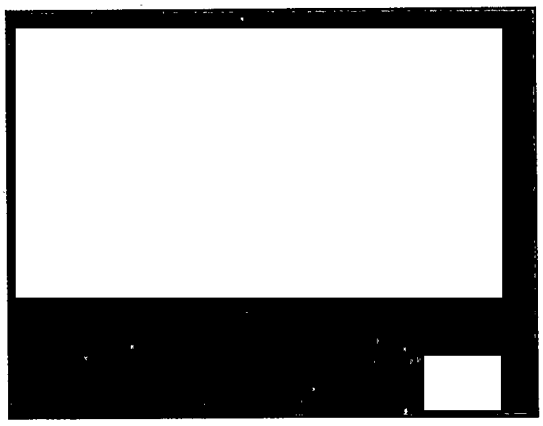


b7E

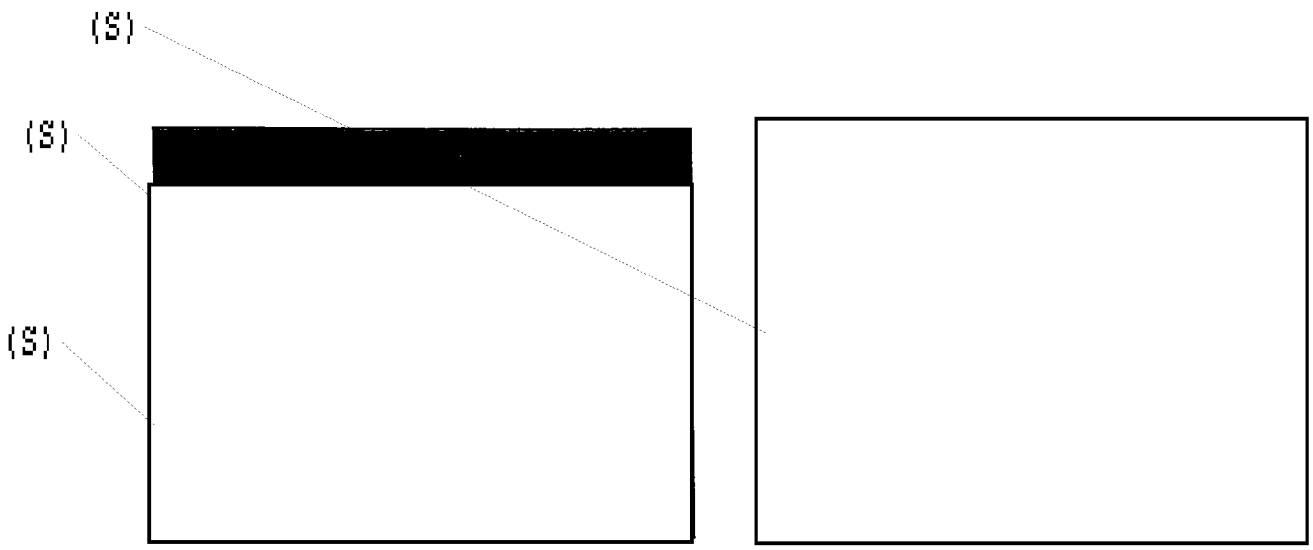
(S)

(S)

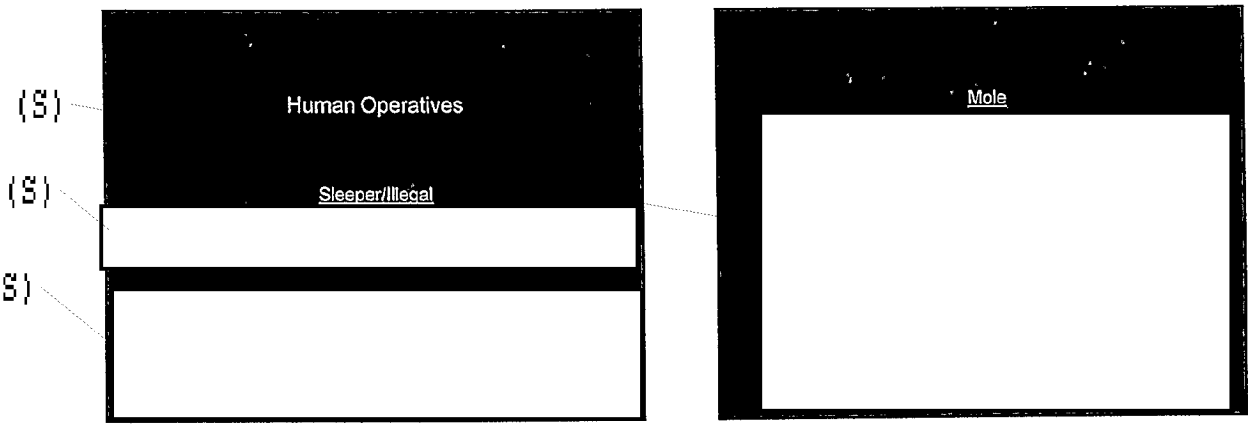




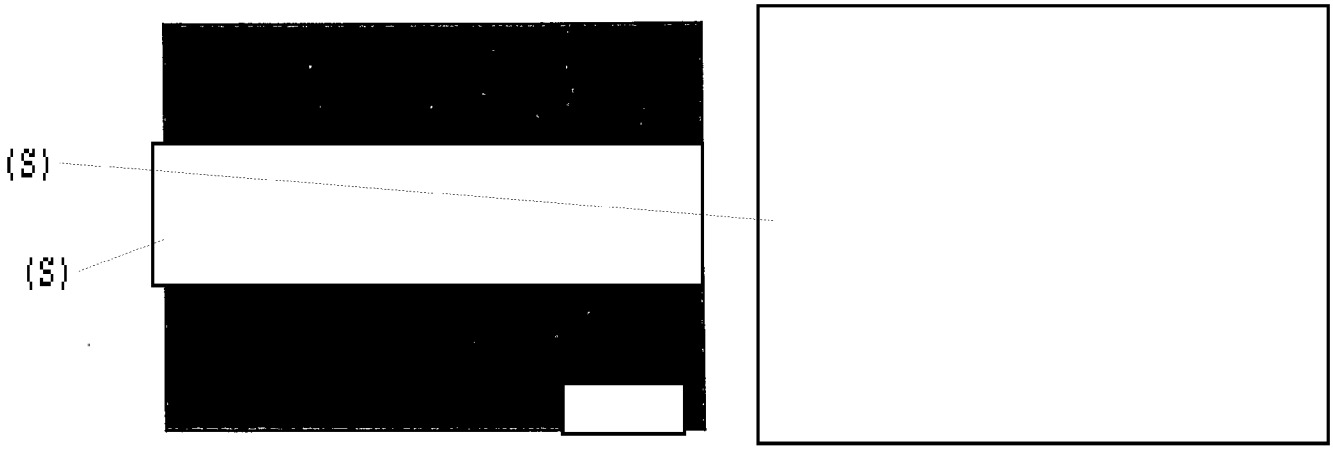
b1
b7E



b1
b7E



b1
b7E



b1
b7E

ACLURM032292

(S)

Clandestine Electronic Devices

b1
b7E

Listening Devices



b7E

(S)

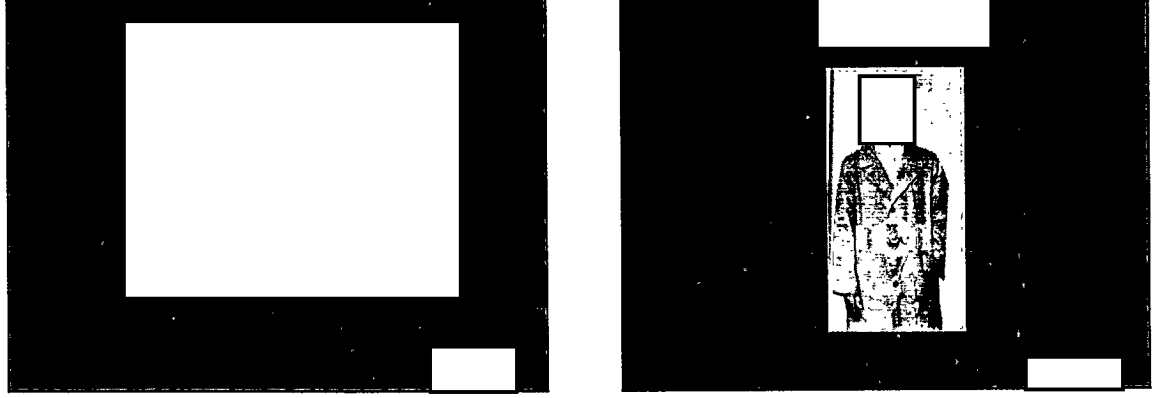
(S)

b1
b7E

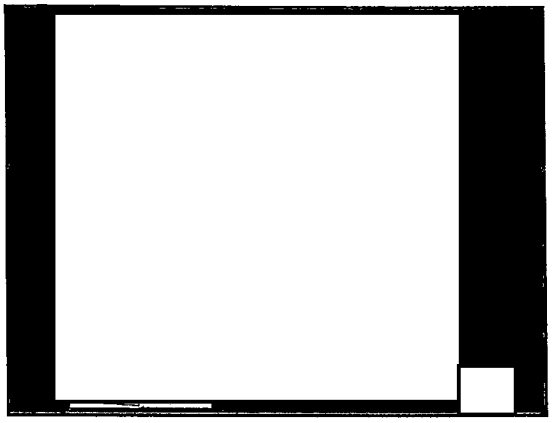
b7E

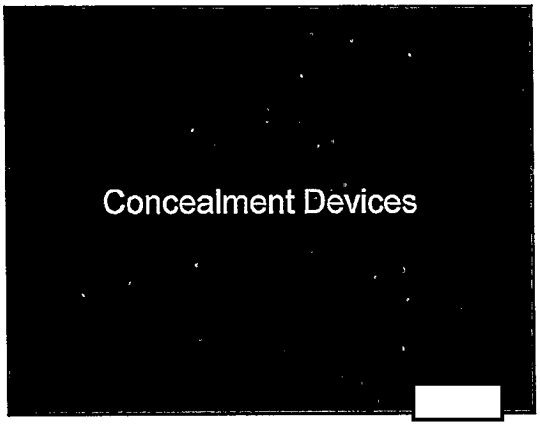
Spy Cameras

b7E

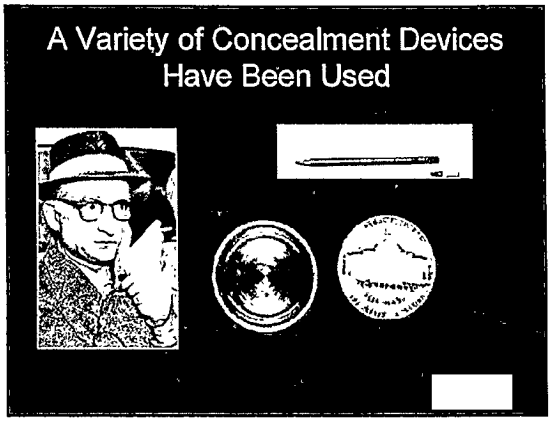


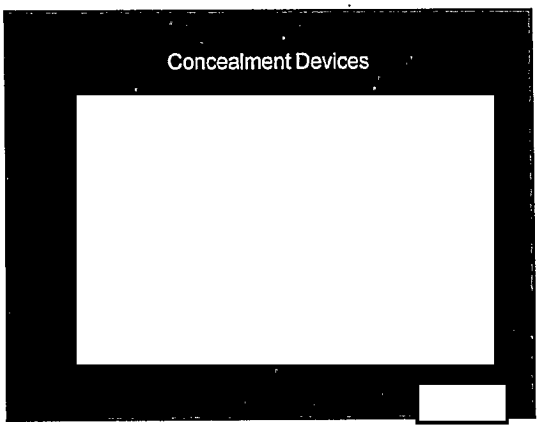
b6
b7C
b7E



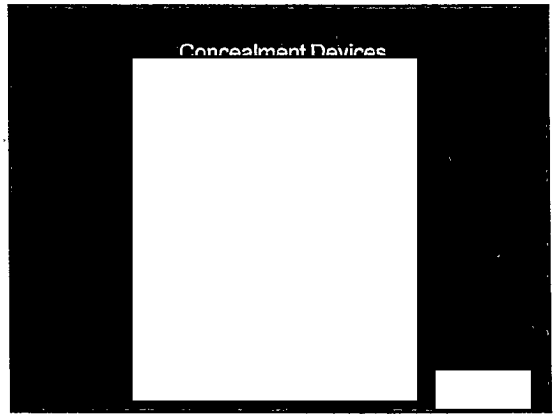

Concealment Devices

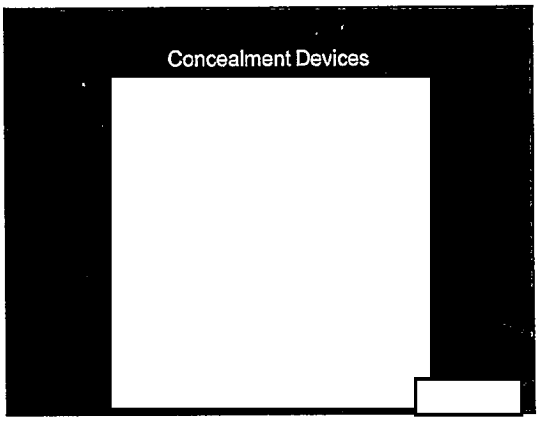
b7E


A Variety of Concealment Devices
Have Been Used

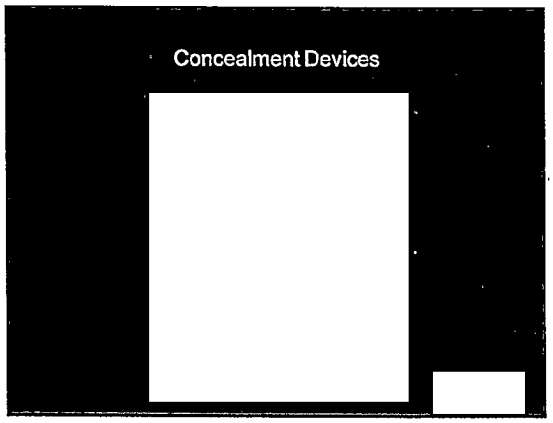

Concealment Devices

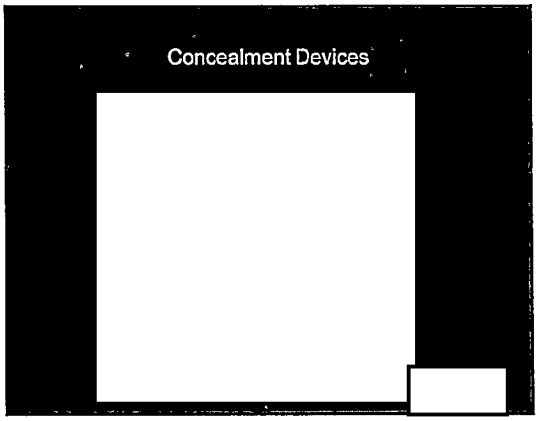
b7E


Concealment Devices

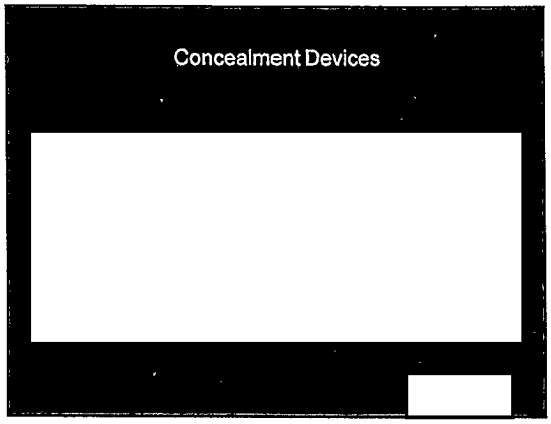

Concealment Devices

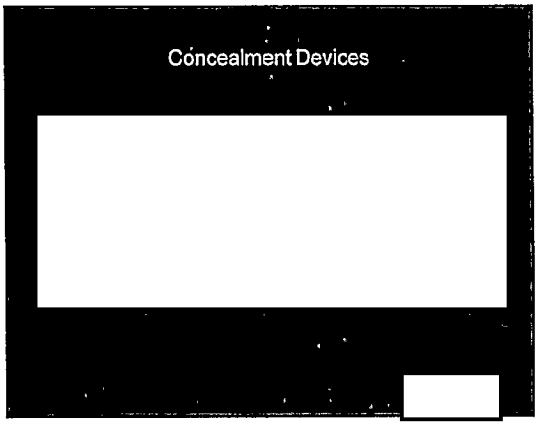
b7E





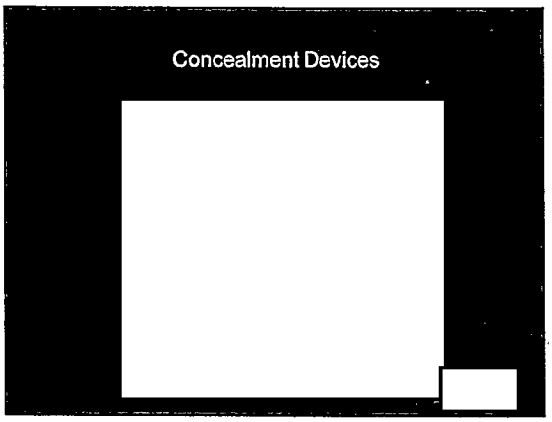
b7E

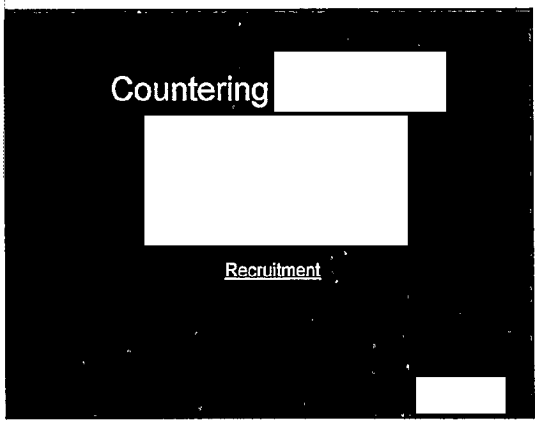




b7E

(S)



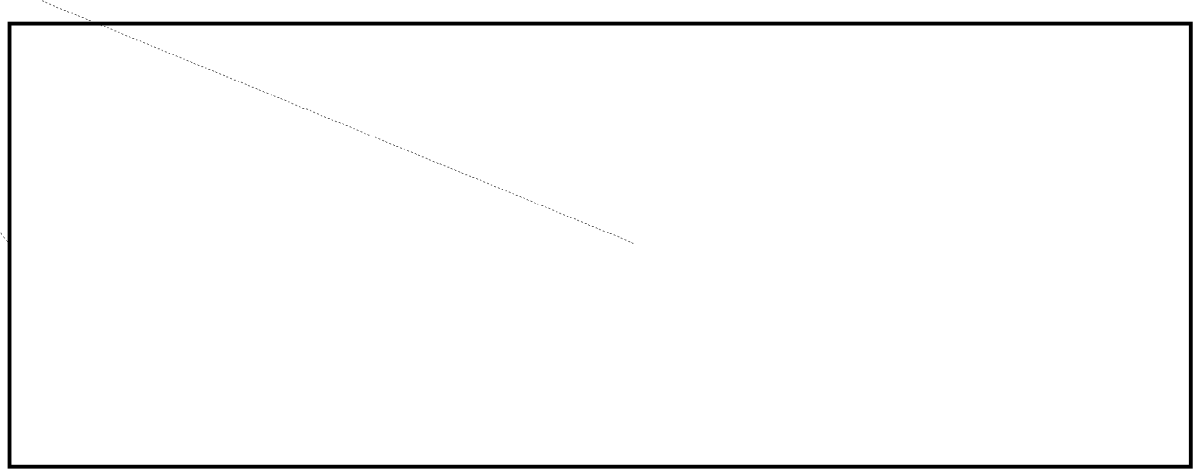


b1
b7E

ACLURM032296

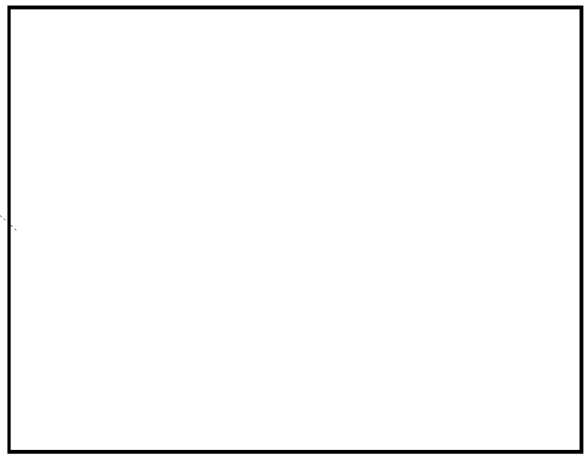
(S)

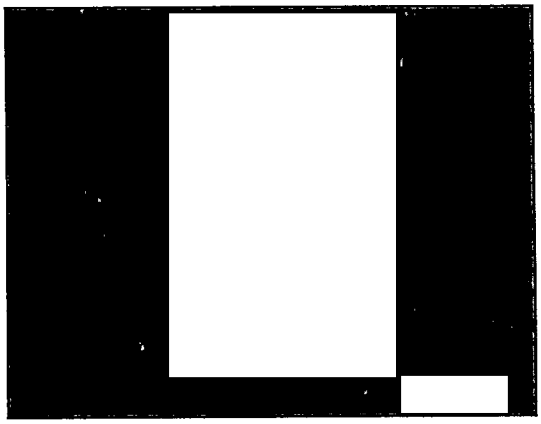
(S)



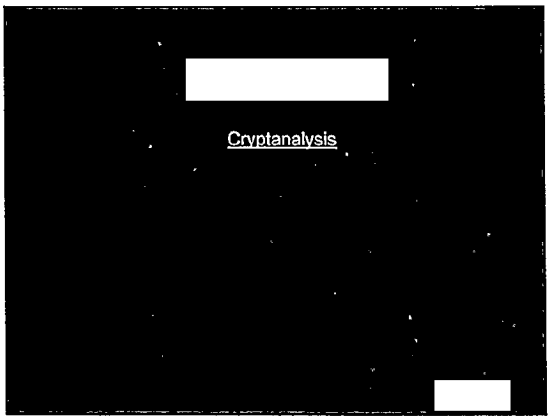
b1
b7E

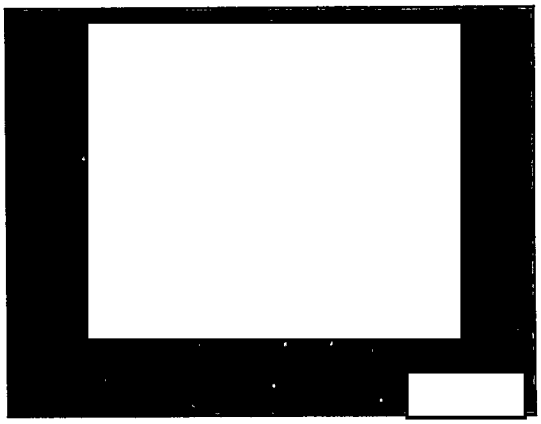
(S)





b1
b7E





b7E

Video

b7E

(S)

Lockouts and Surveillance





SURVEILLANCE

b1
b7E

SURVEILLANCE

(S)

Listening Devices

b1
b7E



b7E

Federal Bureau of Investigation

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-07-2012 BY 65179/DMH/BAW/STP/bls

Title of Instruction: Contemporary [redacted] b6 b7C b7E

Time of Instruction: Two (2) Hours

Target Group: FBI Special Agents and other selected personnel

Instructor: [redacted]

Method of Instruction: Lecture

Additional Information: None

June 6, 2006.

Lesson Plan

Contemporary [redacted]

Slide #	*Teaching Points/Comments*
1	Introductory Slide.
2	**Comment** Agenda for presentation. See slide. b7E
3	**Teaching Point** Provide student a definition of "[redacted]" **Comment** [redacted]
4	**Teaching Point** [redacted] b7E **Comment** In the final days of the Cold War, the crumbling Soviet Union possessed the nuclear weapons to destroy the world but lacked the economic and informational infrastructure to compete as a world power. While the preeminent weapon for most of this century was the hydrogen bomb, it

has been replaced by the awesome capability of a single electron! Future superpowers will be those nations with the greatest capability to harness the power of the electron for both economic and "digital" warfare.
The desire of foreign spies to uncover and obtain "military secrets" will continue, but with variations. We are witnessing the migration of a national defensive infrastructure that has historically been based on "bullets" into one based upon "information." Success by spies targeting an opponent's "information" will ultimately prove more valuable.
New technologies are changing the traditional methods and techniques, the [redacted] by which spies operate.
1
http://www.cnn.com/SPECIALS/cold.war/experience/spies/melton.essay/ b7E

5 **Teaching Point**

With the end of the Cold War, the strong East vs. West alignment in the world has diminished leading to a redefinition of intelligence based on national interests.

Comment

Even at the height of Cold War solidarity (the enemy of my enemy is my friend), the major superpowers collected intelligence and attacked the ciphers, or codes, of our friends as well as our enemies. The national interests of former friends and foes are now being redefined in terms of competing economic interests.

Some observers believe that cultural and historic friendships between nations will continue to fade as they are replaced by trading partnerships and other interdependent economic relationships. The friend of my enemy may also be my friend -- if the price is right. Military alliances will be designed to protect, perpetuate and enhance underlying economic partnerships. The victors in global economic warfare will form regional economic alliances that will share information and together strengthen their collective -- and individual -- economic power.

Gen. Yuri Kobaladze of the SVR -- the Russian Foreign Intelligence Service, successor to the First Chief Directorate of the KGB -- recently stated "there are friendly nations, but there are no friendly intelligence services". [1]

1 http://www.cnn.com/SPECIALS/cold.war/experience/spies/ melton.essay/

6 **Teaching Point**

The traditional methods of collecting and communicating intelligence have changed in ways that could not be imagined just a few years ago.

Comment

The following outlines some technology advances that have dramatically impacted intelligence services' methods:

[redacted] b7E

ACLURM032301
FBI031821

b7E

[redacted]

7 **Teaching Point**

In some important ways, espionage agents can accomplish certain tasks using modern technology that previously required great personal risk.

Comment

[redacted]

b7E

ACLURM032302
FBI031822

b6
b7C
b7E

[redacted]

8 **Teaching Point**

Profound changes in technology have dramatically affected the methods employed to communicate to and from espionage agents.

Comment

[redacted]

b7E

9 **Teaching Point**

To acquaint the student with use of malware by hostile intelligence services.

Comment

Disruption of the enemy's capabilities has long been a goal of intelligence services.

Wikipedia defines "malware" as software designed to infiltrate or damage a computer system, without the owner's informed consent. The term is a portmanteau of "mal-" (or perhaps "malicious") and "software", and describes the intent of the creator, rather than any particular features. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and some adware. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of California, West Virginia, and several other U.S. states.[1]

In the new world of the digital spy, these same activities can be accomplished, at no personal risk, from a computer terminal thousands of miles away. By digitally sabotaging enemy computer networks, cyber-spies can accomplish the same result as their OSS and SOE predecessors. The vulnerability of the national information infrastructure of most countries -- the interlocking computer networks that regulate communication, commerce and defense -- make Pearl Harbor in 1941 appear well protected. At the same time, billions of dollars are being spent to shore up unprotected computer networks, and accelerated programs are being developed to exploit the computer networks of our enemies as we prepare for future "cyber wars."

Computer viruses have been developed and deployed that will be activated in time of war. Imagine the consequence of embedding a "Trojan horse" in the operating system software that runs 90 percent of

ACLURM032303
FBI031823

b7E

the computers of both friends and foes. A "Trojan horse," once activated, can selectively disable the computer infrastructure of a hostile opponent and cripple its economy, communications and defense. The war is over before it has begun.

1 http://en.wikipedia.org/wiki/Malware

10 **Comment**

Slide provides outline of what will be covered. Note that only a general description of the technique will be provided as the lecturer is not an engineer.

11 **Teaching Point**

Acquaint students with a computer virus and its potential impact.

Comment

See slide and next two slides.

A virus is a self-replicating/self-reproducing-automation program that spreads by inserting copies of itself into other executable code or documents.

12 **Comment**

Virus

The infected file (or executable code that is not part of a file) is called a "host". Viruses generally do not affect network performance, as their malicious activities are mostly confined within the target computer itself.

Viruses are one of the several types of malicious software or malware

Predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

13 **Comment**

[redacted]

b7E

14 **Teaching Point**

Acquaint students with a computer worm and its potential impact.

Comment

See this slide and next slide.

Pictured is Sven Jaschan who was arrested near Rotenberg, Germany, on May 8. He subsequently confessed to creating the Sasser worm. The 18-

ACLURM032304
FBI031824

year-old was apprehended following a tip to Microsoft Corp. from a group of people in the culprit's home state of Lower Saxony.

The Wikipedia defines the **Sasser worm** as a computer worm that affects computers running vulnerable versions of the Microsoft operating systems Windows XP and Windows 2000. Like other recent worms, Sasser spreads by exploiting the system through a vulnerable network port.

The effects of Sasser include the news agency *Agency France-Presse* (AFP) having all its satellite communications blocked for hours and the U.S. flight company Delta Air Lines having to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm.[1]

1 http://en.wikipedia.org/wiki/Sasser_worm

15 **Comment**

Worms

They are often designed to exploit the file transmission capabilities found on many computers.

The main difference between a computer virus and a worm is that a virus cannot propagate by itself whereas worms can.

A worm uses a network to send copies of itself to other systems and it does so without any intervention.

In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer.

16 **Teaching Point**

To acquaint the student with the concept of the Trojan horse program.

Comment

Trojan horse programs cannot operate autonomously, in contrast to some other types of malware, like viruses or worms. Just as the Greeks needed the Trojans to bring the horse inside for their plan to work, Trojan horse programs depend on actions by the intended victims. As such, if trojans replicate and even distribute themselves, each new victim must run the program/trojan. Therefore their virulence is of a different nature, depending on successful implementation of social engineering concepts rather than flaws in a computer system's security design or configuration.

17 **Teaching Point**

To acquaint the student with the concept of the Trojan horse program.

Comment

Two common types of Trojan horses:

1. Corrupting useful software, a cracker inserts malicious code that

executes while the program is used.

Examples: weather alerting programs, computer clock setting software, and peer to peer file sharing utilities.

1. Masquerading standalone program as something else
    1. Examples: Using a game or image file to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

18 **Teaching Point**

To acquaint the student with the technique of computer spoofing and its potential use by an intelligence service.

Comment

From the FBI website: "IP Spoofing" is a technique used to gain unauthorized access to computers, whereby the intruder sends a message to a computer with an IP address indicating that the message is coming from a trusted port.

Spoofing is generally used as a means to convince individuals to provide personal or financial information that enables the perpetrators to commit credit card/bank fraud or other forms of identity theft. Spoofing also often involves trademark and other intellectual property violations.

[redacted] b7E

19 **Teaching Point**

To acquaint the student with the technique of computer phishing and its potential use by an intelligence service.

Comment

According to Computer World, phishing isn't really new -- it's a type of scam that has been around for years and in fact predates computers. Malicious crackers did it over the phone for years and called it social engineering. What is new is its contemporary delivery vehicle -- spam and faked Web pages.

Phishing (sometimes called carding or brand spoofing) uses e-mail messages that purport to come from legitimate businesses that one might have dealings with -- banks such as Citibank; online organizations such as eBay and PayPal; Internet service providers such as AOL, MSN, Yahoo and EarthLink; online retailers such as Best Buy; and insurance agencies. The messages may look quite authentic, featuring corporate logos and formats similar to the ones used for legitimate messages. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. [1]

1 See http://www.computerworld.com/securitytopics/security/story/0,

b7E

10801,89096,00.html

20 **Teaching Point**

To acquaint the student with the technique of computer phishing and its potential use by an intelligence service.

Comment

The following from the *Washington* Post, (By Brian Krebs | February 13, 2006; 1:50 PM ET). A source recently forwarded a link to one of the "best" phishing attacks I've ever seen. This one -- targeting the tiny **Mountain America** credit union in Salt Lake City, Utah -- arrives in an HTML-based e-mail telling recipients that their Mountain America credit union card was automatically enrolled in the Verified by Visa program, a legitimate security program offered by Visa that is supposed to provide "reassurance that only you can use your Visa card online."

The e-mail includes the first five digits of the "enrolled card," but those five digits are found on all Mountain America bank cards, so that portion of the scam is likely to be highly convincing for some recipients. The message directs readers to click on a link and activate their new Verified by Visa membership.

Now here's where it gets really interesting. The phishing site, which is still up at the time of this writing, is protected by a Secure Sockets Layer (SSL) encryption certificate issued by a division of the credit reporting bureau **Equifax** that is now part of a company called **Geotrust**. SSL is a technology designed to ensure that sensitive information transmitted online cannot be read by a third-party who may have access to the data stream while it is being transmitted. All legitimate banking sites use them, but it's pretty rare to see them on fraudulent sites.

21 **Teaching Point**

To acquaint the student with the technique of monitoring the use of computers.

Comment

[redacted]

b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 56
Page 25 ~ b1, b6, b7C, b7E
Page 46 ~ b1, b7E
Page 49 ~ b1, b7E
Page 50 ~ b1, b7E
Page 51 ~ b1, b7E
Page 53 ~ b1, b7E
Page 54 ~ b1, b7E
Page 55 ~ b1, b7E
Page 58 ~ b1, b7E
Page 59 ~ b1, b7E
Page 63 ~ b1, b7E
Page 64 ~ b1, b7E
Page 65 ~ b1, b7E
Page 67 ~ b1, b7E
Page 68 ~ b1, b7E
Page 70 ~ b1, b7E
Page 71 ~ b1, b7E
Page 72 ~ b1, b7E
Page 73 ~ b1, b7E
Page 75 ~ b1, b7E
Page 76 ~ b1, b7E
Page 87 ~ Duplicate
Page 88 ~ Duplicate
Page 89 ~ Duplicate
Page 90 ~ Duplicate
Page 179 ~ b1, b7E
Page 180 ~ b1, b7E
Page 181 ~ b1, b7E
Page 185 ~ b1, b7E
Page 186 ~ b1, b7E
Page 187 ~ b1, b7E
Page 188 ~ b1, b7E
Page 189 ~ b1, b7E
Page 190 ~ b1, b7E
Page 191 ~ b1, b7E
Page 193 ~ b1, b7E
Page 194 ~ b1, b7E
Page 195 ~ b1, b7E
Page 196 ~ b1, b7E
Page 197 ~ b1, b7E
Page 241 ~ Duplicate
Page 242 ~ Duplicate
Page 243 ~ Duplicate
Page 340 ~ b1, b7E

Page 341 ~ b1, b7E
Page 368 ~ b6, b7C
Page 386 ~ Duplicate
Page 387 ~ Duplicate
Page 388 ~ Duplicate
Page 391 ~ Duplicate
Page 392 ~ Duplicate
Page 393 ~ Duplicate
Page 399 ~ Duplicate
Page 400 ~ Duplicate
Page 431 ~ b1, b7E
Page 435 ~ b7E