

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-09-2012 BY 65179 DMH/STW

DISCOVERY REQUEST MATERIAL

MANAGING COUNTERINTELLIGENCE INVESTIGATIONS & OPERATIONS (CIOPs) COURSE

AUGUST 20-24, 2007 (07-02)
OCTOBER 29 - NOVEMBER 2, 2007 (08-01)
MAY 19-23, 2008 (08-02)
JUNE 22-26, 2009 (09-01)

~~SECRET~~



Managing Counterintelligence Investigations & Operations

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)

August 20-24, 2007

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Monday, August DECLASSIFY ON: 02-09-2037

7:45 am - 8:15 am

Welcome to Counterintelligence

UC [redacted] CITC
SSA [redacted] CITC

b6
b7C

8:15 am - 10:00 am

Attorney General Guidelines for National Security Investigations

[redacted] Office of the General Counsel

10:00 am - 10:10 am

Break

10:10 am - 12:00 pm

*Foreign Intelligence Surveillance Act and Intelligence Oversight
Board Issues*

[redacted] Office of the General Counsel

12:00 pm - 1:00 pm

Lunch

1:00 pm - 2:50 pm

[redacted] Validation and
what to do when [redacted] ...
SSA [redacted] CITC

b6
b7C
b7E

2:50 pm - 3:00 pm

Break

3:00 pm - 4:50 pm

Espionage
SSA [redacted] CITC

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

August 20-24, 2007

Tuesday, August 21st

7:45 am - 8:00 am

Administrative Issues

8:00 am - 8:50 am

[redacted]
SSA [redacted] CITC

9:00 am - 9:10 am

Break

9:10 am - 10:50 am

[redacted] A Case Study
SSA [redacted] CITC

10:50 am - 11:00 am

Break

11:00 am - 1:00 pm

Working Lunch: CD Resources

SSA [redacted] OSIC/Special Projects
SSA [redacted] Physical Surveillance
SSA [redacted]

(S)

1:00 pm - 2:00 pm

Statistics

[redacted] Retired SSA, Counterintelligence Division

2:00 pm - 2:10 pm

Break

2:10 pm - 3:10 pm

FIGs in the Field

SSA [redacted] Richmond Division

3:10 pm - 3:20 pm

Break

3:20 pm - 4:00 pm

Intelligence Community Requirements

IA/RO [redacted]

4:00 pm - 4:10 pm

Break

4:10 pm - 5:00 pm

Overseas Operations

SSA [redacted] CITC

b1
b6
b7C
b7E

b6
b7C

Managing Counterintelligence Investigations & Operations

~~SECRET~~

FBI042008

~~SECRET~~



August 20-24, 2007

Wednesday, August 22nd

7:45 am - 8:00 am

Administrative Issues

8:00 am - 8:50 am

The FBI's Counterintelligence Strategy

[Redacted] Retired SSA, Tampa Division

8:50 am - 9:00 am

Break

9:00 am - 9:50 am

Interfacing with the Domain

[Redacted] Retired SSA, Tampa Division

9:50 am - 10:00 am

Break

10:00 am - 10:50 am

Domain Contacts

[Redacted] Retired SSA, Tampa Division

10:50 am - 11:00 am

Break

11:00 am - 11:50 am

Engaging in Strategic Partnerships

[Redacted] Retired SSA, Tampa Division

11:50 am - 1:00 pm

Lunch

1:00 pm - 1:50 pm

Engaging in Strategic Partnerships

[Redacted] Retired SSA, Tampa Division

1:50 pm - 2:00 pm

Break

2:00 pm - 2:50 pm

Understanding the Threat

[Redacted] Retired SSA, Tampa Division

2:50 pm - 3:00 pm

Break

3:00 pm - 3:50 pm

Conducting Sophisticated Operations

[Redacted] Retired SSA, Tampa Division

3:50 pm - 4:00 pm

Break

4:00 pm - 4:50 pm

Identifying and Investigating the Threat in Your Domain

[Redacted] Retired SSA, Tampa Division

b6
b7C

Managing Counterintelligence

~~SECRET~~ Investigations & Operations

ACLURM043109

FBI042009

~~SECRET~~



August 20-24, 2007

Thursday, August 23rd

7:45 am - 8:00 am

Administrative Issues

8:00 am - 9:50 am



Interacting in the Business and Academic Domain
Guest Speaker

9:50 am - 10:00 am

Break

10:00 am - 11:30 am

Working with  *partners*

LTC
SSA
SSA



b6
b7C
b7D
b7E

11:30 am - 12:30 pm

Lunch

(S) 12:30 pm - 1:30 pm



b1
b6
b7C
b7E

1:30 pm - 1:40 pm

Break

1:40 pm - 2:40 pm

CI Investigations and the Cyber Threat

SSA



Cyber Division

2:40 pm - 2:50 pm

Break

2:50 pm - 3:50 pm

Counterproliferation

SSA



b6
b7C
b7E

3:50 pm - 4:00 pm

Break

4:00 pm - 5:30 pm

SSA Roundtable Discussion

Managing Counterintelligence Investigations & Operations

~~SECRET~~

August 20-24, 2007

ACLURM043110

Friday, August 24th

7:45 am - 8:00 am

Administrative Issues

8:00 am - 9:00 am

Executive Presentation

DAD John Slattery, Counterintelligence Division

9:00 am - 9:30 am

Evaluations and Wrap-Up

~~SECRET~~

Counterintelligence Training Center						7/13/2011		
Please complete this form to to insure training credit is recorded.								
Class Name:				TR#		Virtual Academy: yes or no		
Travel Dates:						* required information -		
Class Dates:								
Class Location:								
Class Coordinator:				Section/Unit Sponsor:				
Notes:								
*	*			*	*	*		
Last Name	First Name	Preferred	MI	Title	SSN	FO	Telephone	Notes

b6
b7C

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

MCIOPs 07-02 (Aug)

Field Offices EC sent to:	Field Office Candidate	Status
----------------------------------	-------------------------------	---------------

--

b6
b7C

(S)

USIC Partners

--

b1
b6
b7C
b7E

Others wishing to attend:

--

b6
b7C

~~SECRET~~

~~SECRET~~

20-24)

(S)

b1
b7E

~~SECRET~~

~~SECRET~~

MCIOPs 07-02 (Aug 20-24)			
Field Offices EC sent to:	Field Office Candidate	Status	
USIC Partners			
Others wishing to attend:			
Canceled/Withdrawn/Other			

b6
b7C

b1
b6
b7C
b7E

b6
b7C

b6
b7C
b7E

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 200

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FBI Attendees

Telephone Number

--

b6
b7C

USIC Attendees

--

b6
b7C
b7E

James W. Gayhart
SSA-Section Chief
Diplomatic Security Service
Department of State

(571) 345-7516

~~SECRET~~

~~SECRET~~

USIC Attendees

Telephone Number

(S)

b1
b6
b7C
b7E

Thomas M. Tyndall
Section Chief
Far East Region
Counterintelligence Field Activity

(703) 699-7509

~~SECRET~~

~~SECRET~~

Counterintelligence Training Center								10/29/2007
Please complete this form to [redacted] to insure training credit is recorded.								
Class Name:	MCIOPS				TR# 14DV080503			
Travel Dates:	10/28/2007 and 11/02/2007							
Class Dates:	10/29 - 11/02/2007							
Class Location:	[redacted]							
Class Coordinator:	[redacted]				Section/Unit Sponsor:		[redacted]	
Notes:								
*	*			*	*	*		
Last Name	First Name	Preferred	MI	Title	SSN	FO/Agency	Telephone	Lodging

b6
b7C
b7E

b1
b6
b7C
b7E

(S)

[redacted]

~~SECRET~~

~~SECRET~~

Last Name	First Name MI	Title	SSN	FO	CourseID
-----------	---------------	-------	-----	----	----------

(S)

(S)

b1
b6
b7C
b7E

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 10/24/2007

Date: 10/11/2007

To: Counterintelligence
Albany
Boston
Houston
Indianapolis
Jacksonville
Los Angeles
New York
Richmond
San Francisco
Seattle
Washington Field

Attn: CI Program Managers
Training Coordinators

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-09-2012 BY 65179 DMH/STW

From: Counterintelligence
CI Training Center [redacted] Rm 4634
Contact: SSA [redacted]
[redacted]

b6
b7A
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted] kd

Case ID #: [redacted] (Pending)

Title: MANAGING COUNTERINTELLIGENCE INVESTIGATIONS
AND OPERATIONS COURSE 08-01;
COUNTERINTELLIGENCE DIVISION;
COUNTERINTELLIGENCE TRAINING CENTER;
OCTOBER 29 - NOVEMBER 2, 2007
DEADLINE: OCTOBER 24, 2007

Synopsis: Advises invited Field Offices of the captioned mandatory training course.

Reference: [redacted]

b7A
b7E

Details: Referenced EC mandates the Managing Counterintelligence Investigations and Operations Course (MCIOPS) for all Field Office Supervisory Special Agents (SSA) [redacted]

[redacted] In order to meet this mandate, the CD's Counterintelligence Training Center (CITC) is conducting an MCIOPS course from October 29 - November 2, 2007, [redacted]
[redacted]

To: Counterintelligence
From: Counterintelligence
Re: [REDACTED] 10/11/2007

Albany

b7A

The MCIOPS course is a foundation for managing CI investigations and operations. It is the supervisory equivalent to the four-week Counterintelligence Investigations and Operations Course (CIOPS) for SAs newly assigned to CI. This course is primarily for those SSAs [REDACTED] It is also considered a career enhancing course and therefore, acting SSAs and relief supervisors will not be selected to attend. The CIOPS course is designed to address the CI needs of acting SSAs and relief supervisors.

b7E

Once the field deadline has passed (10/24/2007), this course will be open to CD SSAs who wish to attend. CD SSAs should follow the same registration procedures, as detailed below, and will be notified of their selection to attend no later than 10/25/2007.

The web-based Introduction to Counterintelligence course, located on the Virtual Academy, is [REDACTED] for attendance at the MCIOPS course.

b7E

The MCIOPS is a one-week course covering a wide variety of CI program matters including, but not limited to, CI investigative objectives, conducting threat assessments, CI operational techniques, paperwork, [REDACTED] utilized by intelligence services, and briefings from both FBI Headquarters operational entities and other U.S. Government agencies.

The MCIOPS course is neither a replacement for nor an equivalent to the Training Division, Management Sciences Unit, Field Supervisory Course, which is designed for new field supervisors and covers administrative matters concerning supervising a field office squad, regardless of program.

Administrative information regarding this course is as follows:

COURSE LOCATION AND DURATION:

The MCIOPS course will be held at [REDACTED]
[REDACTED] This one-week course will begin promptly at 7:45 am on Monday morning, 10/29/2007, and will end at 9:45 am on Friday morning, 11/2/2007. Sunday, 10/28/2007, is the designated travel day for this course. This in-service will have evening assignments, activities and study sessions and attendees are expected to attend and participate in all sessions. Return airline reservations should be scheduled for departure no earlier than 1:00 p.m. on Friday afternoon, 11/2/2007.

b7E

To: . Counterintelligence
From: Counterintelligence
Re: [REDACTED] 10/11/2007

Albany

b7A

VOUCHERS:

Vouchers for travel to and from this conference will be charged to a TR # which will be provided at a later date. Rental cars are authorized under this TR number.

TRAVEL AND TRANSPORTATION:

Personnel attending this course should be aware that Dulles International Airport (IAD) is the closest airport [REDACTED]
[REDACTED] Attendees may fly into IAD or Ronald Reagan Washington National Airport (DCA) if traveling by air.

b7E

ACCOMMODATIONS:

Each attendee is responsible for making his/her own hotel reservations. The following hotels have advised they currently have government rate rooms available:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

b7E

To: Counterintelligence
From: Counterintelligence
Re: [REDACTED] 10/11/2007

Albany

b7A

[REDACTED]

[REDACTED] All of these hotels are [REDACTED]

b6
b7C
b7E

ATTENDANCE:

As is customary at in-services, attendance is mandatory for all course sessions. Absences for reasons of illness and/or emergency may be authorized by the course directors but other absences must be approved by the CITC Unit Chief, [REDACTED] who can be reached at [REDACTED] and your Field Office ASAC. This requirement is to ensure the attendee is in an on-duty status and thus protect the attendee's rights in the event of accident or death.

REGISTRATION:

FBI Virtual Academy (FBIVA) and FBI e-mail will be the mechanisms to register for the class. CITC requests attendees complete the following:

(1) Complete entry in FBIVA and have your supervisor and training technician approve training; and

(2) Via internal FBI e-mail to [REDACTED] (CD), using the subject "MCIOPS COURSE 08-01," provide the following information:

b6
b7C

- a) Official Bureau Name and title
- b) Preferred name for classroom name strip
- c) SSAN
- d) Bureau EOD, CI EOD
- e) Investigative priority(ies) assigned
- f) Cell phone number
- g) Selected lodging site

COURSE LOCATION AND INFORMATION:

Because this course is being held at [REDACTED] each attendee will be required to complete a non-disclosure statement. Details regarding the location of [REDACTED] parking facilities, and other arrival information will be provided to each student upon receipt of his/her registration information.

b7E

TURK:

To: Counterintelligence
From: Counterintelligence
Re: [REDACTED] 10/11/2007.

Albany

b7A

In accordance with the FY 2008 FBI Investigative Classifications Guide, CI training received is TURKed as 1I. Since proper TURK affects Availability Pay, Agents should ensure attendance at in-services is placed in the proper TURK category.

MISCELLANEOUS:

Appropriate attire for class will be business casual (collared shirts, slacks, skirts, blouses, etc.).

Any employee who is selected to attend this in-service training and is in need of any reasonable accommodation (i.e., sign language interpreter, audio loop, personal assistant, large print materials, etc.) should contact [REDACTED] immediately upon selection to attend this in-service to provide them with specific needs and/or requirements.

b6
b7C

Questions regarding this course should be directed to the CITC course coordinator, SSA [REDACTED] at [REDACTED]
[REDACTED]

To: Counterintelligence
From: Counterintelligence
Re: [REDACTED] 10/11/2007

Albany

b7A

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

All attendees designated to attend this course should be provided with a copy of this communication. Attendee will complete prerequisites for attendance.

Designated attendees must confirm their attendance of this course via e-mail to [REDACTED] as well as complete entry into Virtual Academy by October 24, 2007. Confirmation e-mail should be titled "MCIOPS 08-01" and include attendee information. b6 b7C

Any Field Office receiving a training slot that it (1) knows it will not be able to fill or, (2) knows that it will not need, should notify the CITC as soon as possible so that standby agents in other Field Offices may be substituted.

♦♦

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 2007

DATE: 02-14-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-14-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Monday, October 29th

7:45 am - 8:00 am

Welcome to Counterintelligence

UC [redacted] CITC (confirmed)
SSA [redacted] CITC (confirmed)

b6
b7C
b7E

8:00 am - 8:50 am

Facility Security Briefing

[redacted] Staff

(S) 9:00 am - 9:50 am

[redacted] (confirmed)

(S) 10:00 am - 10:50 am

[redacted]
IA [redacted] (confirmed)

b1
b6
b7C
b7D
b7E

(S) 11:00 am - 11:50 am

[redacted]
SSA [redacted] CITC (confirmed)
SSA [redacted] CITC (confirmed)

11:50 am - 1:00 pm

Lunch

1:00 pm - 1:50 pm

FIGs in the Field

SSA [redacted] Richmond Division (e-mailed)

b6
b7C
b7E

2:00 pm - 2:50 pm

Intelligence Community Requirements

IA/RO [redacted] (confirmed)

3:00 pm - 4:50 pm

SSA Roundtable Discussion

Guest SSAs (e-mailed; two confirmed)
USIC Partners

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 2007

Tuesday, October 30th

7:45 am - 8:00 am

Administrative Issues

8:00 am - 9:50 am

The FBI's Counterintelligence Strategy

(confirmed)

[REDACTED] Retired SSA, Tampa Division

10:00 am - 10:50 am

Interfacing with the Domain

(confirmed)

[REDACTED] Retired SSA, Tampa Division

11:00 am - 11:50 am

Engaging in Strategic Partnerships

(confirmed)

[REDACTED] Retired SSA, Tampa Division

11:50 am - 1:00 pm

Lunch

1:00 pm - 1:50 pm

Detect, Disrupt, and Deter the "Insider Threat"

(confirmed)

[REDACTED] Retired SSA, Tampa Division

2:00 pm - 2:50 pm

[REDACTED]

b7E

(confirmed)

[REDACTED] Retired SSA, Tampa Division

(S)

3:00 pm - 3:50 pm

[REDACTED]

(confirmed)

[REDACTED] Retired SSA, Tampa Division

(S)

4:00 pm - 4:50 pm

[REDACTED]

(confirmed)

[REDACTED] Retired SSA, Tampa Division

b6
b7C

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 2007

Wednesday, October 31st

7:45 am - 8:00 am

Administrative Issues

8:00 am - 9:50 am

Attorney General Guidelines for National Security Investigations

[redacted] Office of the General Counsel (confirmed)

10:00 am - 11:50 am

Foreign Intelligence Surveillance Act and Intelligence Oversight Board Issues

[redacted] Office of the General Counsel (confirmed)

11:50 pm - 1:00 pm

Lunch

1:00 pm - 1:50 pm

[redacted]

SSA [redacted]

CITC (confirmed)

b6
b7C
b7E

2:00 pm - 3:50 pm

[redacted]

A Case Study

SSA [redacted]

CITC (confirmed)

4:00 pm - 4:50 pm

Espionage

SSA [redacted]

CITC (confirmed)

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 2007

Thursday, November 1st

7:45 am - 8:00 am

Administrative Issues

8:00 am - 8:50 am

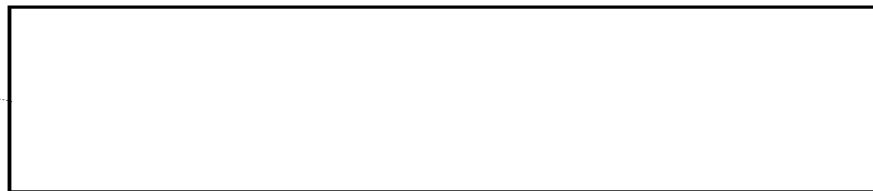
Overseas Operations

SSA [redacted] CITC (confirmed)

9:00 am - 9:50 am

CI Investigations and the Cyber Threat

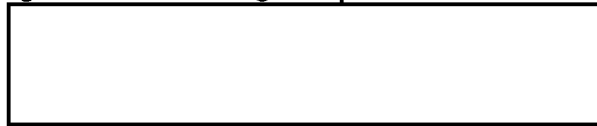
(S) 10:00 am - 10:50 am



b1
b6
b7C
b7E

11:00 am - 1:00 pm

Working Lunch: Working with [redacted] *partners*



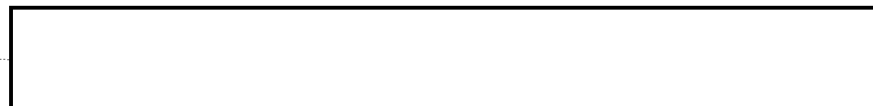
b1
b6
b7C
b7E

1:00 pm - 1:50 pm

Counterproliferation

SSA [redacted]
(confirmed)

(S) 2:00 pm - 2:50 pm



3:00 pm - 3:50 pm

CD Resources

SSA [redacted]
(confirmed)

SSA [redacted] Physical Surveillance
(confirmed)

[redacted] Training (confirmed)

b6
b7C
b7E

4:00 pm - 4:50 pm

[redacted] *Validation*
SSA [redacted] CITC (confirmed)

~~SECRET~~

~~SECRET~~



Managing Counterintelligence Investigations & Operations

October 29 - November 2, 2007

Friday, November 2, 2007

7:45 am - 8:00 am

Administrative Issues

8:00 am - 9:00 am

Executive Presentation

DAD John Slattery, Counterintelligence Division

(confirmed)

9:00 am - 9:30 am

Evaluations and Wrap-Up

~~SECRET~~

~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



Managing Counterintelligence Investigations and Operations

May 19 - 23, 2008

Attendees

Agency

Telephone Number

--

b1
b6
b7C
b7E

Robert P. Hayes, Commander, Deputy Director USCG-Washington, DC

--

b6
b7C

~~SECRET~~

ACLURM043131

FBI042031

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 05/09/2008

Date: 04/09/2008

To: All Field Offices
Counterintelligence

Attn: CI Program Managers
Training Coordinators

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-09-2012 BY 65179 DMH/STW

From: Counterintelligence
CI Training Center [redacted] Rm 4634
Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: MANAGING COUNTERINTELLIGENCE INVESTIGATIONS
AND OPERATIONS COURSE 08-02;
COUNTERINTELLIGENCE DIVISION
COUNTERINTELLIGENCE TRAINING CENTER;
MAY 19-23, 2008
DEADLINE: MAY 9, 2008

Synopsis: Advises Counterintelligence Division and Field Offices
of the captioned mandatory training course.

Reference: [redacted]

Details: Referenced EC mandates the Managing Counterintelligence
Investigations and Operations Course (MCIOPS) [redacted]

[redacted] In order to
meet this mandate, the CD's Counterintelligence Training Center
(CITC) [redacted]

[redacted]

[redacted]

b6
b7A
b7C
b7E

b7A
b7E

b7E

To: ?? From: Counterintelligence
Re: [REDACTED] 04/09/2008

b7A

[REDACTED]

Once the field deadline has passed (05/09/2008), this course will be open to CD SSAs who wish to attend. CD SSAs should follow the same registration procedures, as detailed below, and will be notified of their selection to attend no later than 05/13/2008.

The web-based Introduction to Counterintelligence course, located on the Virtual Academy, is [REDACTED] for attendance at the MCIOPS course.

b7E

The MCIOPS is a one-week course covering a wide variety of CI program matters including, but not limited to, CI investigative objectives, conducting threat assessments, CI operational techniques, paperwork, [REDACTED] utilized by intelligence services, and briefings from both FBI Headquarters operational entities and other U.S. Government agencies.

The MCIOPS course is neither a replacement for nor an equivalent to the Training Division, Management Sciences Unit, Field Supervisory Course, which is designed for new field supervisors and covers administrative matters concerning supervising a field office squad, regardless of program.

Administrative information regarding this course is as follows:

COURSE LOCATION AND DURATION:

The MCIOPS course will be held at [REDACTED]
[REDACTED] This one-week course will begin promptly at 7:45 am on Monday morning, 05/19/2008, and will end at 9:45 am on Friday morning, 05/23/2008. Sunday, 05/18/2008, is the designated travel day for this course. This in-service will have evening assignments, activities and study sessions and attendees are expected to attend and participate in all sessions. Return airline reservations should be scheduled for departure no earlier than 1:00 p.m. on Friday afternoon, 05/23/2008.

b7E

To: ?? From: Counterintelligence
Re: [REDACTED] 04/09/2008

b7A

VOUCHERS:

Vouchers for travel to and from this conference will be charged to TR # 14DV080504 Rental cars are authorized under this TR number.

TRAVEL AND TRANSPORTATION:

Personnel attending this course should be aware that Dulles International Airport (IAD) is the closest airport [REDACTED] [REDACTED] Attendees may fly into IAD or Ronald Reagan Washington National Airport (DCA) if traveling by air.

b7E

ACCOMMODATIONS:

Each attendee is responsible for making his/her own hotel reservations. The following hotels have advised they currently have government rate rooms available:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b7E

To: ?? From: Counterintelligence
Re: [REDACTED] 04/09/2008

b7A

All of these hotels are [REDACTED]
[REDACTED]

ATTENDANCE:

As is customary at in-services, attendance is mandatory for all course sessions. Absences for reasons of illness and/or emergency may be authorized by the course directors but other absences must be approved by the CITC Unit Chief, [REDACTED] [REDACTED] who can be reached at [REDACTED] and your Field Office ASAC. This requirement is to ensure the attendee is in an on-duty status and thus protect the attendee's rights in the event of accident or death.

b6
b7C
b7E

REGISTRATION:

FBI Virtual Academy (FBIVA) and FBI e-mail will be the mechanisms to register for the class. CITC requests attendees complete the following before 05/09/2008:

(1) Complete entry in FBIVA and have your supervisor and training technician approve training; and

(2) Via internal FBI e-mail to [REDACTED] [REDACTED] (CD), using the subject "MCIOPS COURSE 08-02," provide the following information:

b6
b7C

- a) Official Bureau Name and title
- b) Preferred name for classroom name strip
- c) SSAN
- d) Bureau EOD, CI EOD
- e) Investigative priority(ies) assigned
- f) Cell phone number
- g) Selected lodging site

COURSE LOCATION AND INFORMATION:

Because this course is being held at a [REDACTED] each attendee will be required to complete a non-disclosure statement. Details regarding the location of the off-site, parking facilities, and other arrival information will be provided to each student upon receipt of his/her registration information.

b7E

TURK:

In accordance with the FY 2008 FBI Investigative Classifications Guide, CI training received is TURKed as 1I.

To: ?? From: Counterintelligence
Re: [REDACTED] 04/09/2008

b7A

Since proper TURK affects Availability Pay, Agents should ensure attendance at in-services is placed in the proper TURK category.

MISCELLANEOUS:

Appropriate attire for class will be business casual (collared shirts, slacks, skirts, blouses, etc.).

Any employee who is selected to attend this in-service training and is in need of any reasonable accommodation (i.e., sign language interpreter, audio loop, personal assistant, large print materials, etc.) should contact [REDACTED] immediately upon selection to attend this in-service to provide them with specific needs and/or requirements.

b6
b7C

Questions regarding this course should be directed to the CITC course coordinator, SSA [REDACTED] at [REDACTED]

To: ?? From: Counterintelligence
Re: [REDACTED] 04/09/2008

b7A

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

All attendees designated to attend this course should be provided with a copy of this communication. Attendee will complete prerequisites for attendance.

Designated attendees must confirm their attendance of this course via e-mail to [REDACTED] as well as complete entry into Virtual Academy by May 9, 2008. Confirmation e-mail should be titled "MCIOPS 08-02" and include attendee information set forth in EC.

b6
b7C

♦♦

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



05/19/2008 – 05/23/2008

b1
b6
b7C
b7E

FBI042038

~~SECRET~~



Managing Counterintelligence Investigations & Operations

June 22 - 26, 2009

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

Attendees

Telephone Number

--	--

(S)

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

MANAGING COUNTERINTELLIGENCE INVESTIGATIONS AND OPERATIONS

June 22-26, 2009

Last Name	First Name Preferred MI	Title	FO/Agency
-----------	-------------------------	-------	-----------

--	--	--	--

b6
b7C
b7E

USIC Partners

(S)

--

b1
b6
b7C
b7E

~~SECRET~~

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Precedence: DEADLINE 06/12/2009

Date: 05/22/2009

To: All Field Offices

Attn: CI Program Managers
Training Coordinators

Counterintelligence

From: Counterintelligence
CI Training Center

Contact: SSA

Approved By:

Drafted By:

kd

Case ID #: (Pending)

Title: MANAGING COUNTERINTELLIGENCE
INVESTIGATIONS AND OPERATIONS COURSE
COUNTERINTELLIGENCE DIVISION
COUNTERINTELLIGENCE TRAINING CENTER
JUNE 22 - 26, 2009

Synopsis: Advises all Field Offices of the captioned mandatory training course.

Details: The Federal Bureau of Investigation (FBI) National Strategy for Counterintelligence (CI) mandates an increased focus on both the professionalization of the FBI CI workforce, and the training required to establish that professionalized cadre. As part of this training, the Counterintelligence Division's (CD) Counterintelligence Training Center (CITC) has developed and mandated the Managing Counterintelligence Investigations and Operations Course (MCIOPs) for all Field Office Supervisory Special Agents (SSA)

The MCIOPs course is a foundation for managing CI investigations and operations. It is the supervisory equivalent to the four-week Counterintelligence Investigations and Operations Course (CIOPs) for SAs newly assigned to CI. This course is primarily for those SSAs It is also considered a career enhancing course and therefore, acting SSAs and relief supervisors will not

UNCLASSIFIED

b6
b7A
b7C
b7E

b7E

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 05/22/2009

b7A

be selected to attend. The MCIOPS course is designed to address the CI needs of acting SSAs and relief supervisors.

Once the field deadline has passed (06/12/2009), this course will be open to CD SSAs who wish to attend. CD SSAs should follow the same registration procedures, as detailed below, and will be notified of their selection to attend no later than 06/16/2009.

The web-based Introduction to Counterintelligence course, located on the Virtual Academy, is [REDACTED] for attendance at the MCIOPS course.

b7E

The MCIOPS is a one-week course covering a wide variety of CI program matters including, but not limited to, [REDACTED]

[REDACTED]

The MCIOPS course is neither a replacement for nor an equivalent to the Training Division, Management Sciences Unit, Field Supervisory Course, which is designed for new field supervisors and covers administrative matters concerning supervising a field office squad, regardless of program.

Administrative information regarding this course is as follows:

COURSE LOCATION AND DURATION:

The MCIOPS course will be held [REDACTED]
[REDACTED] at the FBI Academy. This one-week course will begin promptly at 7:45 am on Monday morning, 06/22/2009, and will end at 9:45 am on Friday morning, 06/26/2009. Sunday, 06/21/2009, is the designated travel day for this course. This in-service will have evening assignments, activities and study sessions and attendees are expected to attend and participate in all sessions. Return airline reservations should be scheduled for departure no earlier than 1:00 p.m. on Friday afternoon, 06/26/2009.

b7E

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 05/22/2009

b7A

VOUCHERS:

Vouchers for travel to and from this conference will be charged to TR51DV090517. Rental cars are not authorized under this TR number. Field Office SACs must approve travel by Bucar.

TRAVEL AND TRANSPORTATION:

Personnel attending this in-service MUST USE Ronald Reagan Washington National Airport (if traveling by air). Free FBI Academy buses will be available. Please consult the Training Division [REDACTED] site for bus times, as they are subject to change. Buses will depart from the bus lane in front of Terminal [REDACTED] Please note that Security at the airport will not allow the buses to sit and wait for students. Therefore, the buses will arrive only a few minutes prior to scheduled departure and depart soon thereafter.

b7E

If a flight delay occurs which causes you to miss the last bus, transportation to the FBI Academy may be facilitated using the DAFRE shuttle service. FYI, Training Division will not reimburse travel to the FBI Academy by any other means. Only the free FBI Academy bus is authorized. Additional information concerning the DAFRE service, as well as costs, may be obtained directly from them at 703-680-0987.

FBI Academy Check-In:

Training Division personnel will be available from 3pm - 9pm on Sunday, June 21, 2009. Arriving students should indicate they are attending a Division 5/Counterintelligence Division course. Student check-in is in an office to the left of the Atrium, in the Jefferson Building. If you are arriving after 9pm, please advise as soon as possible so arrangements can be made for late arrival and badge pick-up.

Due to current per diem regulations, personnel from WFO and FBIHQ who attend this course are not entitled to lodging and meals.

Your badge will grant you access to the CITC space (entry on the [REDACTED])

b7E

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 05/22/2009

b7A
b7E

ATTENDANCE:

As is customary at in-services, attendance is mandatory for all course sessions. Absences for reasons of illness and/or emergency may be authorized by the course directors but other absences must be approved by the CITC Unit Chief, [REDACTED] [REDACTED] who can be reached at [REDACTED] and your Field Office ASAC. This requirement is to ensure the attendee is in an on-duty status and thus protect the attendee's rights in the event of accident or death.

b6
b7C

REGISTRATION:

FBI Virtual Academy (FBIVA) and FBI e-mail will be the mechanisms to register for the class. CITC requests attendees complete the following before 06/12/2009:

(1) Complete entry in FBIVA and have your supervisor and training technician approve training; and

(2) Via internal FBI e-mail to [REDACTED] (CD), using the subject "MCIOPS COURSE 09-01," provide the following information:

b6
b7C

- a) Official Bureau Name and title
- b) Preferred name for classroom name strip
- c) SSAN
- d) Bureau EOD, CI EOD
- e) Investigative priority(ies) assigned
- f) Bureau cell phone/blackberry number

MISCELLANEOUS:

Appropriate attire for class will be business casual (collared shirts, slacks, skirts, blouses, etc.).

All Special Agents are required to bring their Bureau issued weapons [REDACTED]

b7E

Personal laptops and cellular phone with cameras are not allowed in FBI space.

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 05/22/2009

b7A

Any employee who is selected to attend this in-service training and is in need of any reasonable accommodation (i.e., sign language interpreter, audio loop, personal assistant, large print materials, etc.) should contact [REDACTED] immediately upon selection to attend this in-service to provide them with specific needs and/or requirements.

b6
b7C

Questions regarding this course should be directed to the CITC course coordinator, SSA [REDACTED] at [REDACTED]
[REDACTED]

UNCLASSIFIED

UNCLASSIFIED

To: All Field Offices From: Counterintelligence
Re: [REDACTED] 05/22/2009

b7A

LEAD(s) :

Set Lead 1: (Action)

ALL RECEIVING OFFICES

All attendees designated to attend this course should be provided with a copy of this communication. Attendee will complete prerequisites for attendance.

Designated attendees must confirm their attendance of this course via e-mail to [REDACTED] as well as complete entry into Virtual Academy by June 12, 2009. Confirmation e-mail should be titled "MCIOPS 09-01" and include attendee information set forth in EC.

b6
b7C

◆◆

UNCLASSIFIED

~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence Training Center

Please complete this form to [] to insure training credit is recorded.

#####

Class Name: MCIOPS TR# 51DV090517

Travel Dates: 06/21 and 26

Class Dates: 06/22-26/2009

Class Location: CITC classroom

Class Coordinator: []

Section/Unit Sponsor: []

Notes:

Last Name	First Name	Preferred	MI	Title	SSN	FO/Agency	Telephone	Lodging	Cell
-----------	------------	-----------	----	-------	-----	-----------	-----------	---------	------

b6
b7C
b7E

b6
b7C
b7E

USIC Partners

(S)

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



Managing Counterintelligence Investigations and Operations

06/22/2009 – 06/26/2009



Monday, 6/22	Tuesday, 6/23	Wednesday, 6/24	Thursday, 6/25	Friday, 6/26
7:45 am – 8:50 am Admin/Intro/Security SSA [redacted]	7:45 am – 9:50 am OTD SSA [redacted] SSA [redacted] SIA [redacted] IA [redacted]	7:45 am – 8:00 am Administration	7:45 am – 8:00 am Administration	(S) 7:45 am – 9:00 am SSA [redacted]
(S) 9:00 am – 10:00 am CD National Strategy	10:00 am – 11:30 am [redacted] OTD ASC Anthony Gonzalez	8:00 am – 9:30 am SSA [redacted]	8:00 am – 12:00 pm National Security Intelligence Guidelines/ Foreign Intelligence Surveillance Act/ National Security Letters/ Intelligence Oversight Board AGC Craig King	9:00 am Packing and Dismissal
(S) 10:00 am – 11:00 am [redacted] Training Resources	11:30 am – 12:30 am Sensitive Operations OTD UC [redacted]	9:40 am – 10:50 am	12:00 pm – 1:00 pm LUNCH	
11:00 am – 12:00 pm [redacted] Section Acting SC [redacted]	12:30 pm – 1:30 pm LUNCH	11:00 am – 12:00 pm Coordinating CI Investigations Overseas	1:00 pm – 3:30 pm Espionage	
12:00 pm – 1:00 pm LUNCH	1:30 pm – 2:50 pm Undercover Operations (S) SSA [redacted]	12:00 pm – 1:00 pm Lunch		
(S) 1:00 pm – 1:50 pm Global Section UC [redacted]	3:00 pm – 5:00 pm	1:30 pm – 2:00 pm	3:40 pm- 5:00 pm	
2:00 pm – 2:50 pm [redacted] Section [redacted]		2:00 pm – 3:00 pm Counterintelligence Center Counterespionage Group		
3:00 pm – 3:50 pm CI Program Coordination SSA [redacted]	(S)	3:00 pm – 4:00 pm A Day in the Life of a [redacted] Guest Speaker		
4:00 pm – 5:00 pm Counterproliferation SSA [redacted]		4:00 pm – 5:00 pm Cyber CI SSA [redacted]		

b1
b6
b7C
b7D
b7E

b1
b6
b7C
b7D
b7E

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

Time		block name	Instructor, phone #, other	date confirmed	notes
Day 1, Monday July 19					
7:45	8:00	Admin			
8:00	9:00	Introduction by CD Execs			
9:00	9:15	Student introductions Course objectives/ expectations			
9:15	11:30	Running a CI Squad			start out with table tops - will determine who will cover what - will continue 3:30
11:30	12:30	Lunch			
12:30	2:30	National intelligence Integration - CI & FIG			
2:30	3:30	NRO (Proactive initiative re cleared contractors)			
3:30	5:00	(cont) Running a CI Squad			

b6
b7C

Day 2, Tuesday July 20 - Strategic Partners					
8:00	9:00				
9:00	11:00	Military panel	Army -		
		NCIS	NCIS -		
11:00	12:00				left voicemail with 3/11/10
12:00	1:00	Lunch		confirmed	email confirmation
1:00	3:00	Civilian Panel			
3:00	5:00	Internal Partners - In your Division, other FOs, HQ			

b1
b6
b7C
b7Eb6
b7C
b7E

Day 3, Tuesday July 21					
8:00	9:00	Defining Domain		confirmed	
9:00	11:00	Overall Domain Program - Measures for Success			
11:00	12:00	Identifying Presence & Foreign Intelligence Threat	designee		
12:00	1:00	Lunch			
1:00	3:00	FBIHQ Sections: panel			
3:00	5:00	Identifying Presence & Most threatening collectors in Div.			

b6
b7C
b7E~~SECRET~~

~~SECRET~~

(S)

Day 4, Tuesday July 22

8:00	10:00				
(S)		• Sources/CHS • Recruitments • [redacted] • Sophisticated techniques			do we want another speaker or can [redacted] handles this block
(S)		[redacted] Group 1 & Group 2)			
10:00	12:00				
			AUSA		waiting for [redacted] to suggest name
12:00	1:00	Lunch			
		[redacted] Espionage & related			
1:00	2:00	violations			
2:00	3:00	[redacted] Undercover ops			
3:00	5:00	Case presentation			

b1
b6
b7C
b7E

b6
b7C
b7E

b6
b7C
b7E

Day 5, Tuesday July 23

8:00	10:00	Running the Squad follow-up & table top scenarios			Case mentors
10:00		DISMISS			

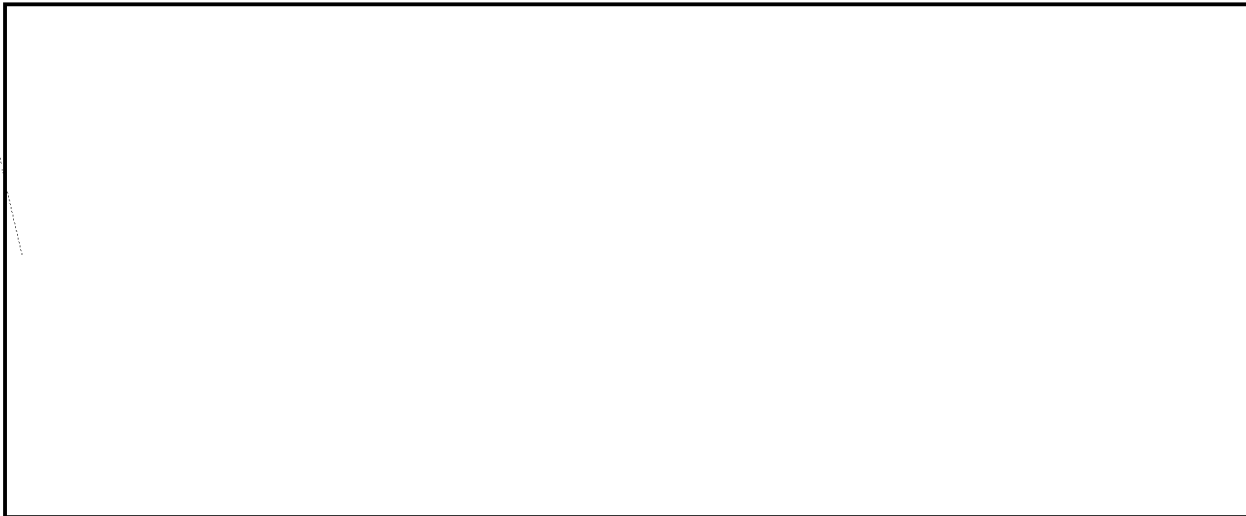
~~SECRET~~

~~SECRET~~

~~SECRET//OC, NF~~

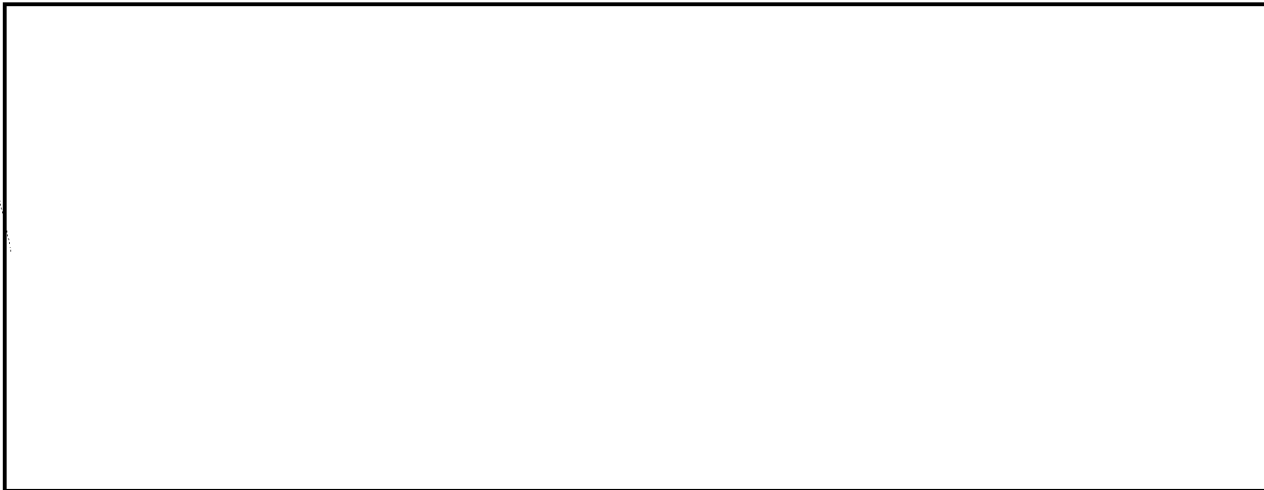
7/13/2011

(S)



b1
b7E

(S)



b1
b7E

(S)



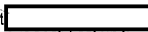
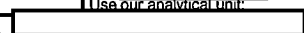
(S)

(S)



Bottom line

- If you have  case and need help, feel free to call HQ
- Keep FBIHQ informed from the start

Questions about 
 Use our analytical unit

~~SECRET//OC, NF~~

36

b1
b6
b7C
b7E

~~SECRET~~

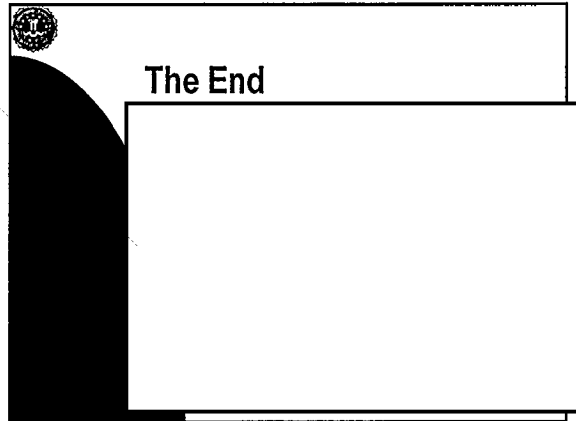
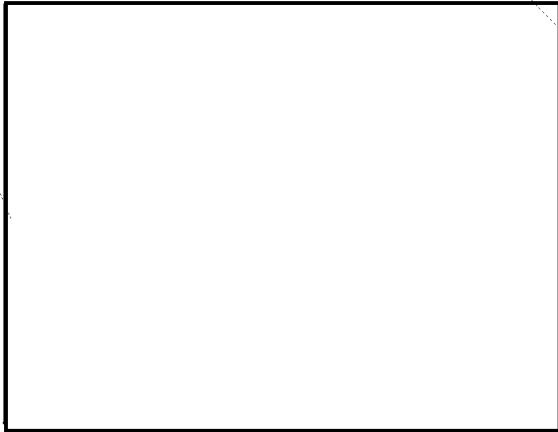
~~SECRET~~

~~SECRET~~//OC, NF

7/13/2011

(S)

(S)



b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



**Federal Bureau of Investigation
Counterintelligence Division**



2002 Counterintelligence Strategy

- ♦ New strategy promulgated August 2002



- It was a first step
- Set the "bar" very high

b7E



2002 Counterintelligence Strategy

- ♦ What precipitated the 2002 strategy?
 - Since 1995 
 - 
 - 
 - 
- Wen Ho Lee and the Bellows Report

(S)

(S)



What Caused the Problems?

1. 

b1
b7E



What Caused the Problems?

2. **Organizational Culture/Attitude**
 - "Those people don't do anything."
 - Using FCI squad as the bench.
 - A place for misfits & problems.
 - Pulling out "good Agents" to do real work.
 - No management support



2002 Counterintelligence Strategy

- ♦ What did the 2002 strategy do?
 - Created central control
 - Helped shift the FBI's organizational culture



b7E

~~SECRET~~



2002 Counterintelligence Strategy

- ♦ When Implemented (con't)
 - Required aggressive [redacted]

[redacted]

- ♦ It would take several years.
- ♦ If we failed, the FBI loses the mission...



2007 Counterintelligence Strategy

- ♦ Builds on the 2002 Strategy
- ♦ Focuses on the top priority threats
- ♦ Focuses on changing the behavior of [redacted]
- ♦ Focuses on changing the behavior of [redacted]
- ♦ Establishes alliances [redacted]

(S)

b1
b7E



2007 Counterintelligence Strategy

- ♦ Regionalizes the [redacted] efforts
- ♦ Reinvigorates and expands the "Insider Threat"
- ♦ Emphasizes proactive collection [redacted]
- ♦ Recognizes the cyber threat, and integrates the cyber program
- ♦ Emphasis on partnerships and information sharing



2007 Counterintelligence Strategy

[redacted]

b7E



Strategic Goals

[redacted] strategic goals prioritize resources and activities.

[redacted]

- ♦ Beyond the ability of one agency
- ♦ Need the cooperation of [redacted]

(S)



Strategic Goal 1

- ♦ Prevent proliferation of WMD, its

[redacted]

b1
b7E



Strategic Goal 2

- ♦ Prevent the penetration of the U.S. Intelligence Community, U S Government agencies and contractors



Strategic Goal 3

- ♦ Prevent the loss or compromise of Critical National Assets, critical US information and technology.

b7E



Strategic Goal 4

- ♦ Enhance



Program Objectives

- ♦ Success will be reflected in the extent to which these objectives are achieved with respect to CI priorities:

b7E



Program Strategies

- ♦ To meet program goals, there are interdependent performance expectations for strategic areas:

(S)



Strategy 1: Interface with the Domain

- ♦ Performance Expectation: Visit and establish liaison with

b1
b7E

 **Strategy 1: Interface with the Domain**

[Redacted]

 **Strategy 2: Engage in Strategic Partnerships**

♦ Performance Expectations:

[Redacted]

b7E

 **Strategy 3: Identify Foreign Intelligence Collection Objectives, Officers, Agents, and Operations**

♦ Performance Expectations:

[Redacted]

■ For both [Redacted] threat

- Identify and understand [Redacted] in your territory
- Identify [Redacted] operations in your territory
- Share information to enhance our knowledge

(S)

(S)

 **Strategy 3: Identify Foreign Intelligence Collection Objectives, Officers, Agents, and Operations**

♦ Performance Expectations:

- Program in place to identify [Redacted]
- Familiar with FBI CI collection requirements [Redacted]
- Conduct annual [Redacted] assessment
- Integrate the CI Program with the FIG

(S)

b1
b7E

 **Strategy 4: Conduct Targeted, High Impact Operations Against Priority Countries**

♦ Performance Expectations:

- All Priority [Redacted] appropriately covered
- Asset base provides quality coverage of both [Redacted] threat
- Develop operations against [Redacted]

(S)

 **Strategy 5: Detect and Deter the Insider Threat**

♦ Performance Expectations:

- Reinvalidate the 811 referral policy
- Close liaison with [Redacted]
- Educate [Redacted]

b1
b7E



Enabling Strategies

- ♦ The ability to implement program strategies is critically dependant upon enhancing:
 - Workforce Expertise
 - Resource Management
 - Intelligence
 - Management Accountability

b7E

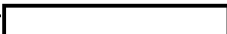


Workforce Expertise

- ♦ Training
- ♦ Continuity
- ♦ Experience



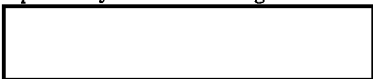
Workforce Expertise

- ♦ Training & Continuity
 - Special Agent Proficiency
 - Advanced training for 
 - 
 - Foster continuity where possible

b7E

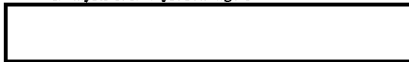


Workforce Expertise

- ♦ Training (Agents and Analysts)
 - Upon entry into the CI Program
 - 
- Annual Continuing Education



Workforce Expertise

- ♦ Continuity & Experience
 - Institutionalize
 - Career Path
 - Agents & Agent Managers
 - Analysts & Analyst Managers
- 

b7E

~~SECRET~~



Resource Management



Intelligence

- ♦ Collection
- ♦ ☐ Base
- ♦ High Quality Analysis

b7E

b7E



Management Accountability

- ♦ Headquarters is responsible for the effective execution of the Program Strategies and Enabling Strategies
- ♦ SACs are responsible for the execution of the Program Strategies within the field divisions



Intelligence

- ♦ High Quality Analysis
 - Threat assessment
 - Support to CD
 - Strategic analytical requirements
 - Tactical analytical requirements
 - Identification of FI and CI information for dissemination

~~SECRET~~

~~SECRET~~



Where are we now?

Implementation Plan



2007 Counterintelligence Strategy Recap

♦ Build on the 2002 Strategy

b7E



S
U
L
T
S

A
C
T
I
V
I
T
I
E
S



QUESTIONS ?

b7E



Counterintelligence Strategy

♦ “Why should I care? “

- Because you came into the FBI to do something important - this is important.
 - The intelligence threat will never go away.
- If you don't understand strategic issues you won't understand how to do your job.
- Strategy is about choices and priorities

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE 11

CI Program Strategy 2007 (S)

ACTIVITIES RESULTS

[Redacted]

[Redacted]

FBI FCI Threat Matrix 2008 -

(S)

[Redacted]

[Redacted]

b1
b7D
b7E

(S)

[Redacted]

(S)

2008 Threat-Based & Issue-Driven Focus:
Limited Resources Means Investigations & Operations
Prioritized Against-

[Redacted]

Prevent	-	WMD Proliferation
Prevent	-	Espionage
Prevent	-	CNA Compromise
Enhance	-	[Redacted]

b1
b7E

~~SECRET~~

~~SECRET~~

DATE: 02-09-2012

CLASSIFIED BY 65179 DMH/STW

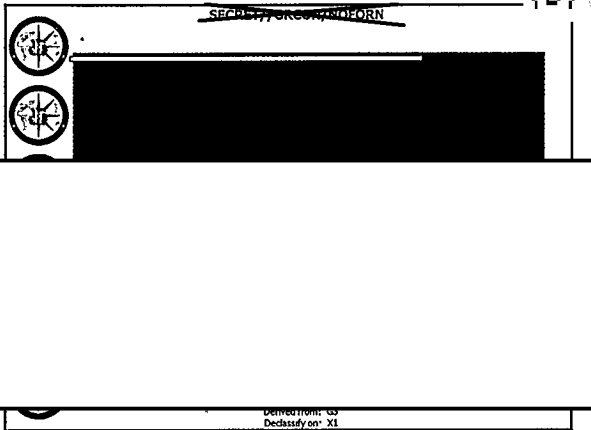
REASON: 1.4 (C)

DECLASSIFY ON: 02-09-2037

~~SECRET~~

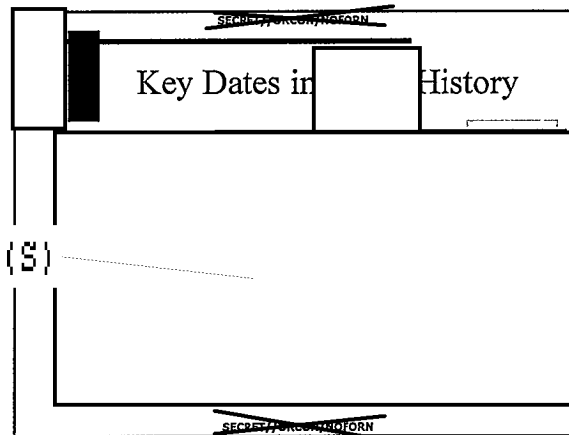
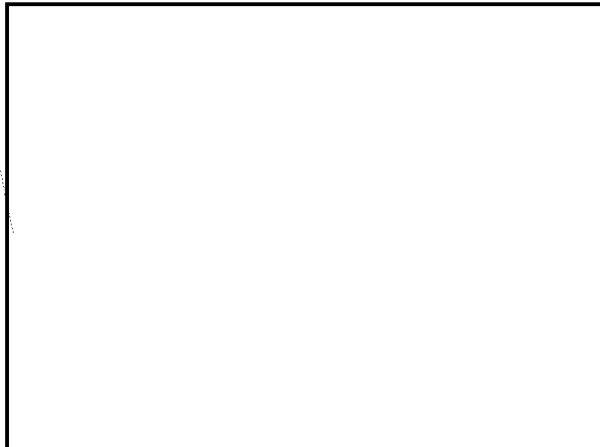
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

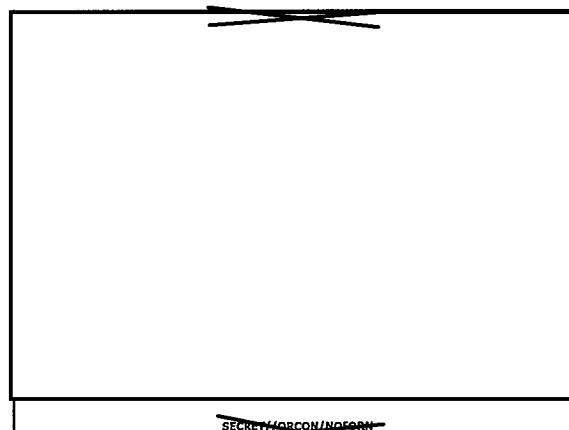
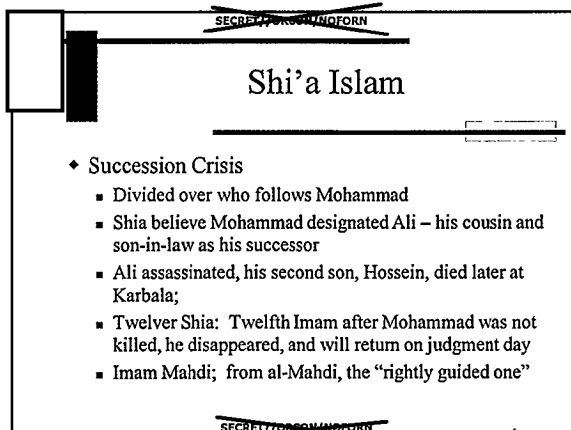


b1
b7D
b7E

(S)



b1
b7D
b7E



b7E

~~SECRET~~

SECRET: Derived from G3, Declassify on
X1

ACLURM043162

~~SECRET~~

~~SECRET//NOFORN~~

Political Philosophy

■ Theoretically, it is within the constitution to replace an individual with a leadership council

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

THE SYSTEM

ELECTED INSTITUTIONS UNELECTED INSTITUTIONS

~~SECRET//NOFORN~~

b7E

(S)

~~SECRET//NOFORN~~

Country Players

(S)

b1
b7D
b7E

(S)

(S)

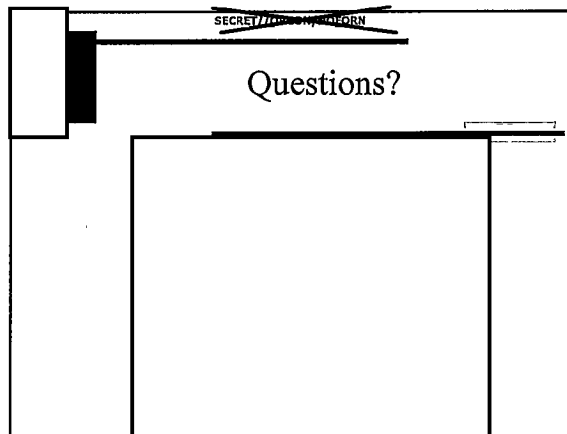
b1
b7D
b7E

~~SECRET~~: Derived from G3, Declassify on X1

ACLURM043163

~~SECRET~~

(S)



b1
b6
b7A
b7C
b7D
b7E

~~SECRET: Derived from G3, Declassify on
X1~~

ACLURM043164

~~SECRET~~DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012**DETECT, DISRUPT, AND
DETER THE "INSIDER
THREAT"****Detect, Disrupt, and Deter the
"Insider Threat"**

- Liaison is established with all U.S. Government Agency security offices
- Provide espionage training to security and management personnel

**Detect, Disrupt, and Deter the
"Insider Threat"**

- Provide security briefings to cleared personnel as in line with resources
- Provide "indicator" training to security and managerial personnel

**Detect, Disrupt, and Deter the
"Insider Threat"**

- Educate security and managerial personnel regarding "anomalies"
- Work with

b7E

**Detect, Disrupt, and Deter the
"Insider Threat"**

- Establish a method to report suspicious activity to the FBI
- Remind Government Agencies of responsibilities under Section 811

**Detect, Disrupt, and Deter the
"Insider Threat"**

- For private industry, liaise with
- Educate Security personnel regarding security indicators

b7E

~~SECRET~~

Detect, Disrupt, and Deter the "Insider Threat"

- Provide briefings to cleared personnel in line with resources

- Integrate [REDACTED]

Detect, Deter, and Disrupt the "Insider Threat"

- Provide a channel to report suspicious activities
- Follow up on all information provided
- Provide feedback as allowed

b7E

~~SECRET~~

7/13/2011

(S)

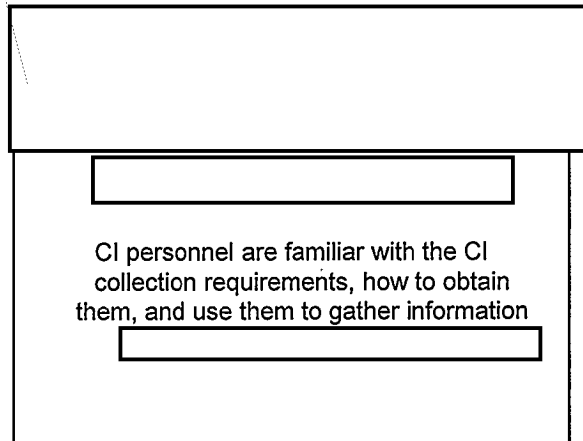


b1
b7E

(S)



(S)



b1
b7E

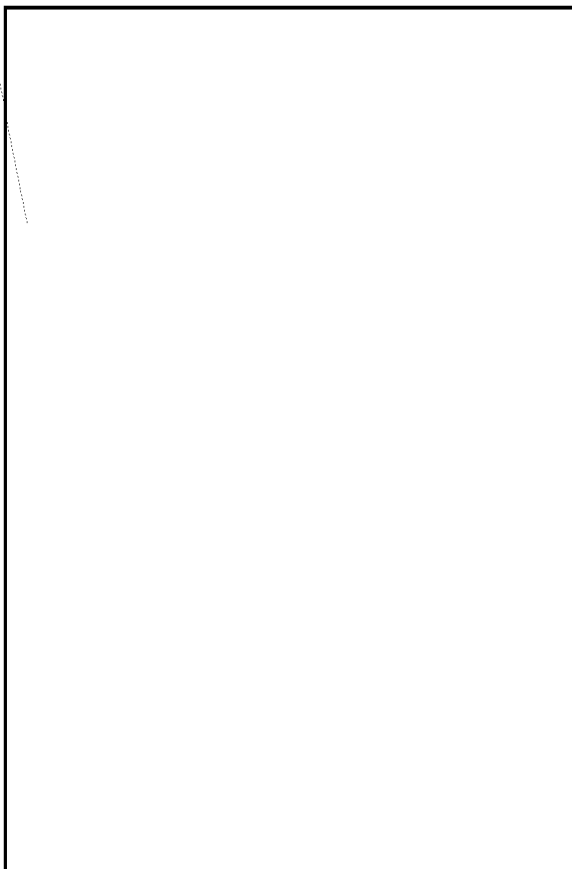
~~SECRET~~

~~SECRET~~

7/13/2011

(S)

(S)



Share information with Strategic Partners to
enhance the FBI's knowledge of [redacted]
[redacted] collection objectives and
activities

b1
b7E

(S)

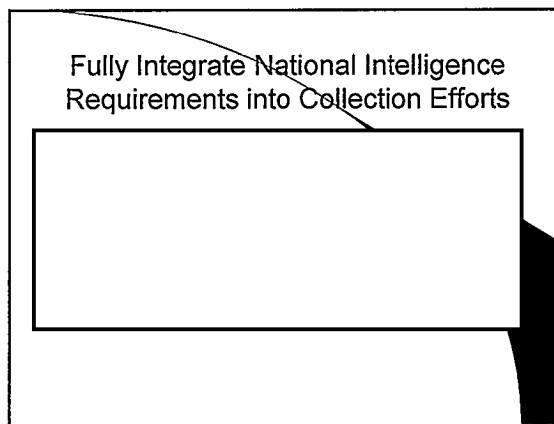
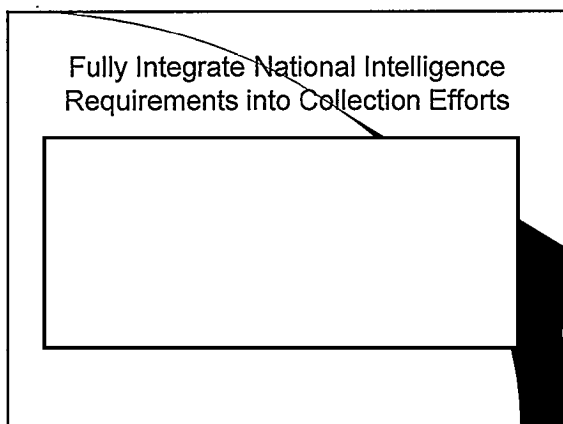
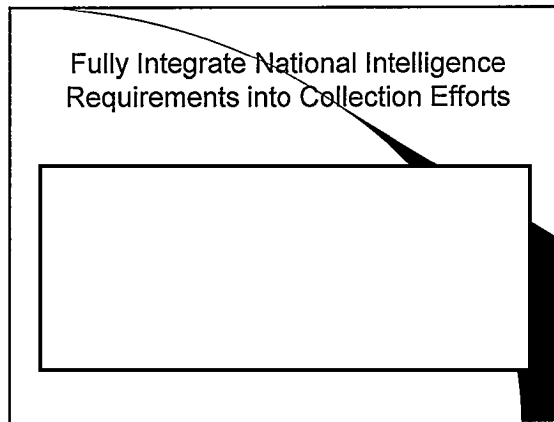
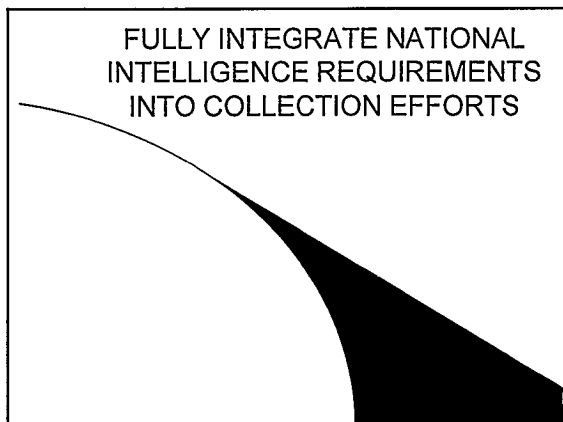


~~SECRET~~

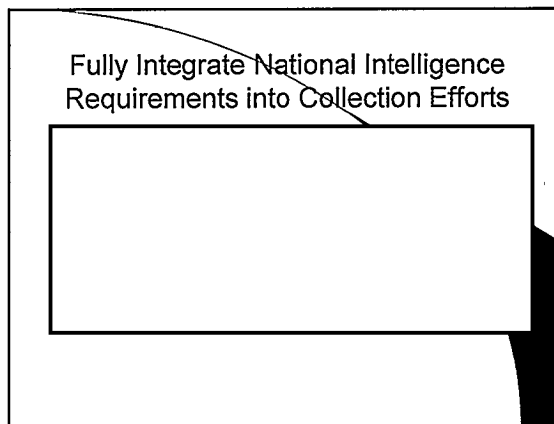
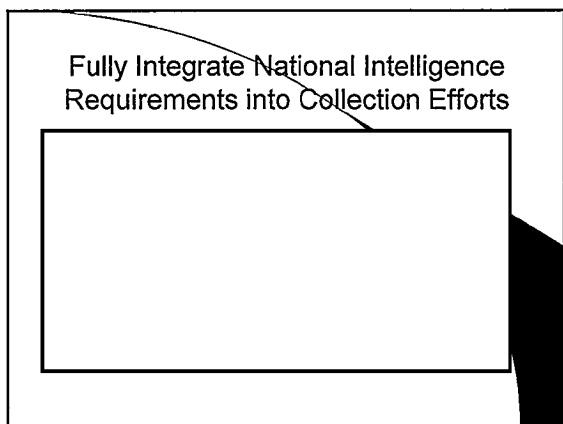
7/13/2011

~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012



b7E



b7E

~~SECRET~~

ACLURM043169

7/13/2011

Fully Integrate National Intelligence
Requirements into Collection Efforts



- CI Analytical products are created and disseminated

b7E

7/13/2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

INTERFACE WITH THE DOMAIN

INTERFACE WITH THE DOMAIN

The Domain:

Anything in the territory that could be of
interest

b7E

INTERFACE WITH THE DOMAIN

(S)

INTERFACE WITH THE DOMAIN

b1
b7E

INTERFACE WITH THE DOMAIN

(S)

INTERFACE WITH THE DOMAIN

Liaison with
Liaison with
Liaison with

b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

INTERFACE WITH THE DOMAIN

CUTTING EDGE

Liaison with

Liaison with

Public Source Information

INTERFACE WITH THE DOMAIN

Liaison with

Liaison with

Liaison with

b7E

INTERFACE WITH THE DOMAIN

> With Strategic Partners. Identify

>

>

>

INTERFACE WITH THE DOMAIN

THE BUSINESS ALLIANCE

Interface with

Provide relevant threat briefings

Introduce the

Establish a means to report suspicious incidents

Schedule meetings and develop a relationship

b7E

INTERFACE WITH THE DOMAIN

FEDERAL AGENCIES WITH

Liaison with

INTERFACE WITH THE DOMAIN

Liaison with

Liaison with

Liaison with

b7E

~~SECRET~~

7/13/2011

INTERFACE WITH THE DOMAIN

[Redacted]

Public Source Information

Liaison with

[Redacted]

INTERFACE WITH THE DOMAIN

> Identify The

[Redacted]

> Why Are They Strategically Important

(S)

> Which [Redacted] is Interested?

b1
b7E

INTERFACE WITH THE DOMAIN

Interface with the

[Redacted]

Provide Relevant Threat Briefings

Inquire About Suspicious Incidents

Identify How Suspicious Incidents Could
Have Intelligence Implications

Schedule Future Meetings and Interaction

INTERFACE WITH THE DOMAIN

With Strategic Partners, Identify the

[Redacted]

Why Are They Strategically Important

(S)

Which [Redacted] is Interested

b1
b7E

INTERFACE WITH THE DOMAIN

(S)

[Redacted]

INTERFACE WITH THE DOMAIN

[Redacted]

What Outreach Efforts Have Been Made
To Help Identify [Redacted] Activity?

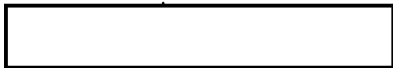
(S)

b1
b7E

~~X~~

7/13/2011

INTERFACE WITH THE DOMAIN



Liaison with

Liaison with

DOMAIN ENTITY INTERVIEW

- WHAT DOES THE ENTITY DO?
- WHY IS IT A TARGET?
- WHY DOES IT NEED TO BE PROTECTED?

b7E

DOMAIN ENTITY INTERVIEW

- Explain the FBI's CI role, responsibilities, and authority
- Explain methodologies
- Define presence
- Explain
- Explain the threat to employees who travel abroad

(S)

DOMAIN ENTITY INTERVIEW

- Explain
- Explain methodologies
- Identify the motivational factors of
- Point out behavioral indicators of

(S)

b1
b7E

DOMAIN ENTITY INTERVIEW

- Determine the major "customers" of the entity
- Obtain information concerning the
- Determine the

DOMAIN ENTITY INTERVIEW

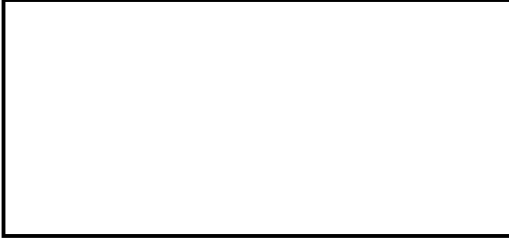
- Determine the identity of
- Determine the number of
- Determine the number of
- Determine if

b7E

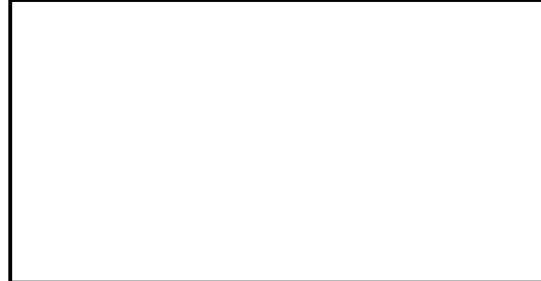
~~SECRET~~

7/13/2011

DOMAIN ENTITY INTERVIEW



DOMAIN ENTITY INTERVIEW

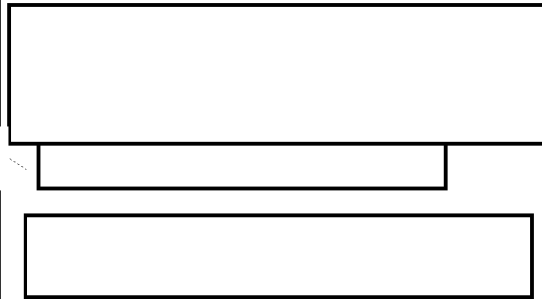


b7E

DOMAIN ENTITY INTERVIEWS



INTERFACE WITH THE DOMAIN



(S)

b1
b7E

~~SECRET~~

~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

Overall Classification of this Presentation:
~~SECRET//NOFORN//CRIMMR~~

(S)

Intelligence Dissemination

Overall Classification of this Presentation:
~~SECRET//NOFORN//CRIMMR~~



b1
b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

The Dilemma...

How can collectors
identify reportable information?

GAPS

"I thought the information
seemed interesting."

"I'd never seen it before.
The information was new
to me."

AND

REQUIREMENTS

"My supervisor said I should
so I thought this
would make for a good one."

"I just gave it to my analyst
and he/she handled it."

Gaps and Requirements

Why should this be important to you?

- The identification of intelligence gaps and the translation of these gaps into intelligence requirements are key steps in providing FBI Agents, Intelligence Analysts and the rest of the community with the best information about the current and future national security threats.

b7E

Gaps and Requirements

What is an intelligence gap?

Any question that identifies a lack of information about a national security issue can be considered an intelligence gap.

Intelligence analysts or program managers normally identify intelligence gaps as they compile and assess information related to:

(S)

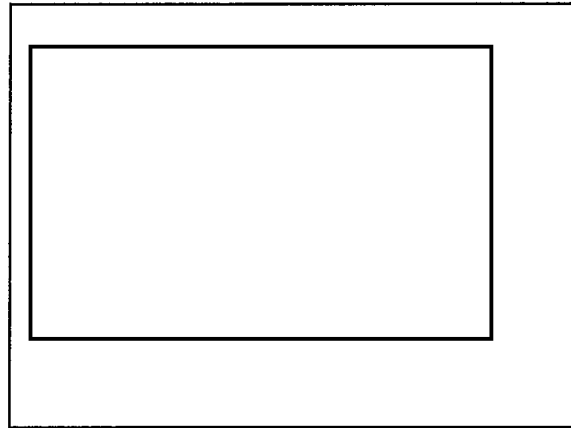
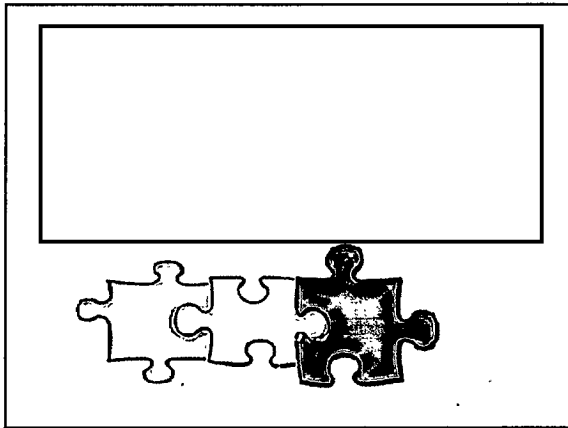
(S)

Intelligence Gap Examples

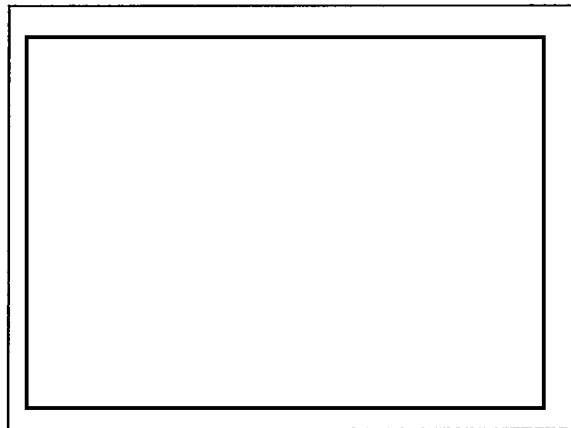
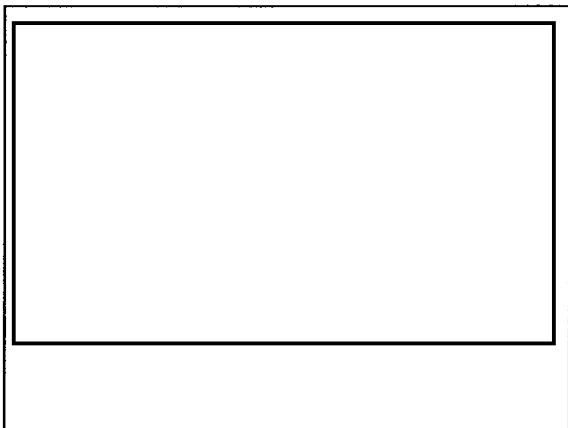
b1
b7D
b7E

~~SECRET~~

~~SECRET~~

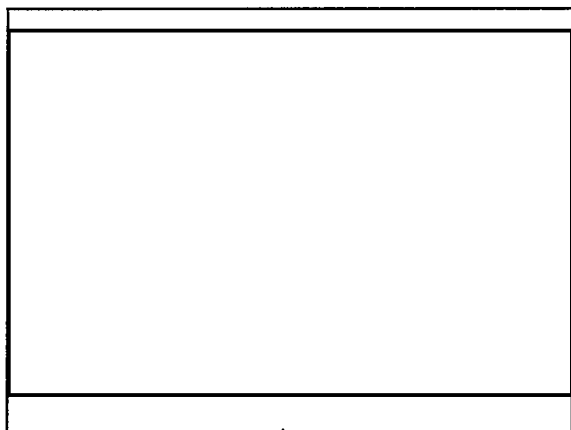


b7E



b7E

How do Requirements Fit Into the
FBI Intelligence Cycle?

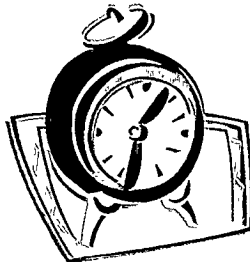


b7E

~~SECRET~~

~~SECRET~~

There's Not Enough Time!



The Solution?



b7E

The Agent/Analyst Relationship

Wow! Let me go and consult the collection requirements!

The source has access to the president's mistress.



Prior to the Asset Debriefing

- Familiarize your Intelligence Analyst with the background (access to information)

- IA provides you with

b7E

During the Asset Debriefing

- Asset provides you with information

Post Asset Debriefing

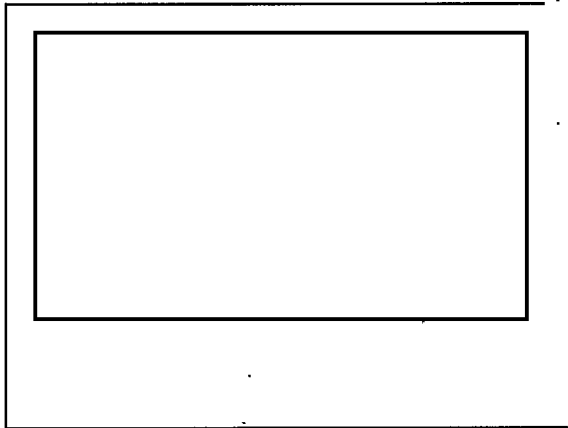
- Talking points answered by the asset should be

b7E

~~SECRET~~

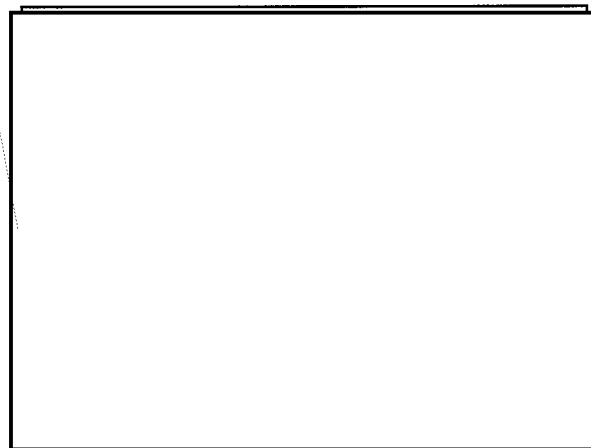
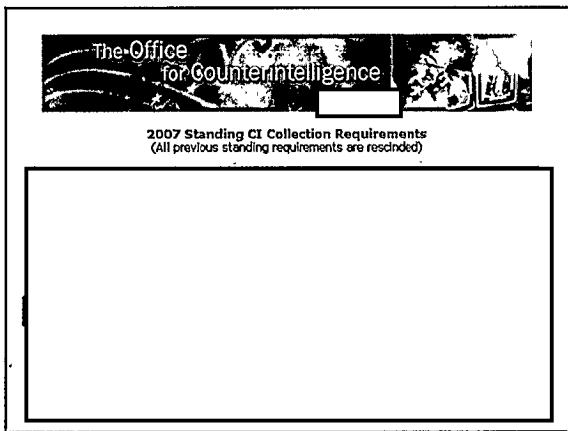
~~SECRET~~

(S)



b1
b7E

(S)



b1
b7E

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

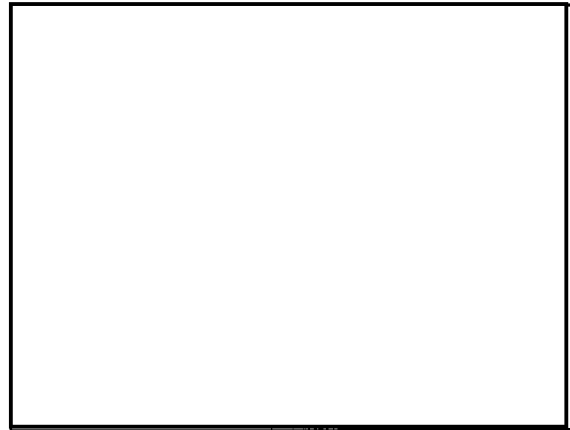
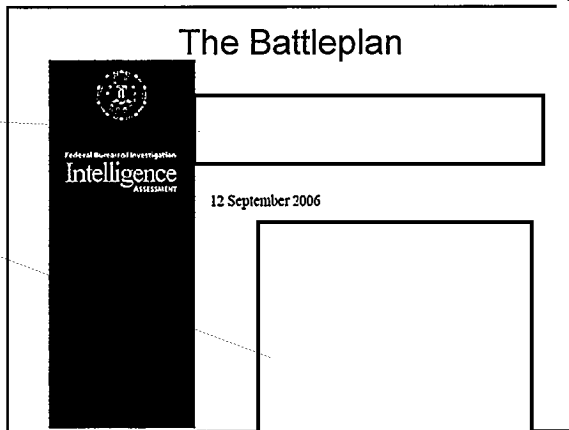
DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

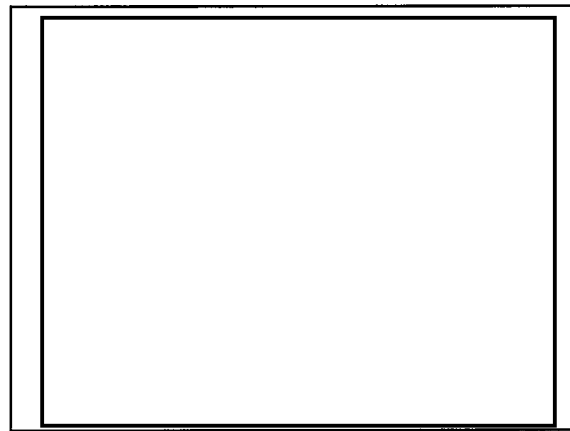
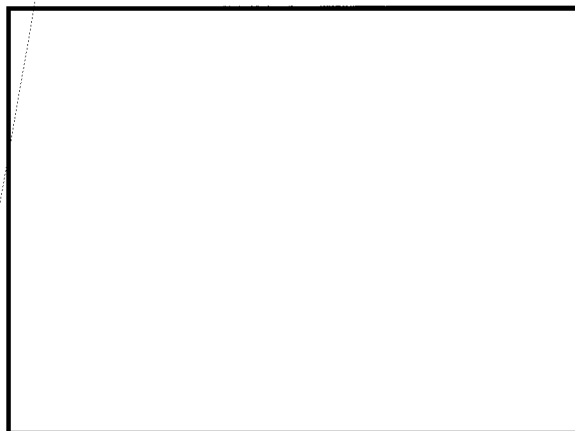
(S)

(S)



b1
b7D
b7E

(S)



b1
b7E

(S)

(S)

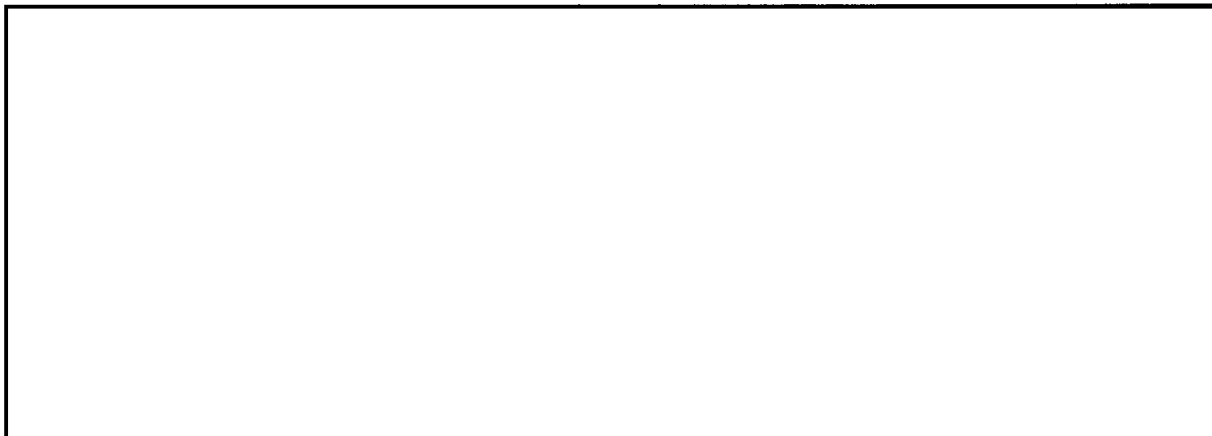


b1
b7D
b7E

~~SECRET~~

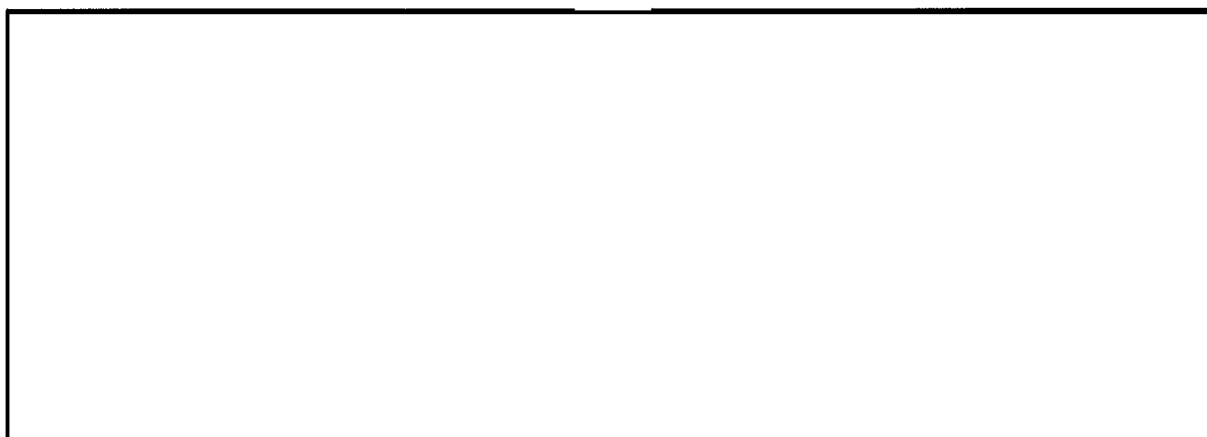
~~SECRET~~

(S)



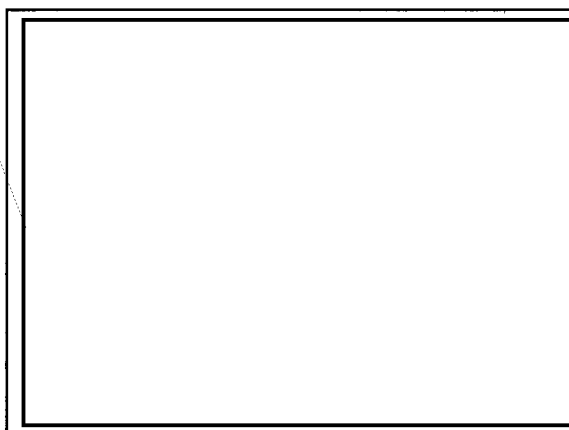
b1
b7D
b7E

(S)



b1
b7D
b7E

(S)



How does the intelligence cycle
benefit the FCI Investigation?

b1
b7E

~~SECRET~~

(S)

In return you get...

- Evaluations of your disseminated [redacted]

[redacted]

- USIC counterparts
- Asset debrief talking points

[redacted] Quality Standards

Outstanding – Well-sourced [redacted]

[redacted]

Excellent – Well-sourced [redacted]

[redacted]

Good – Well-sourced [redacted]

[redacted]

Satisfactory – Report contains [redacted]

[redacted]

b1
b7E

[redacted]

Great Resources...

The [redacted] Focus

b7E

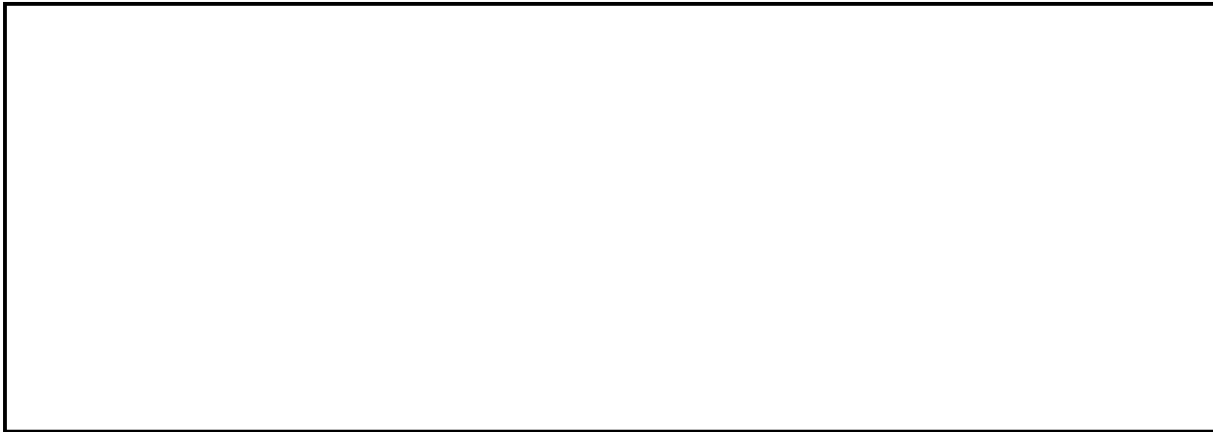
[redacted] Focus Newsletter

[redacted]

[redacted]

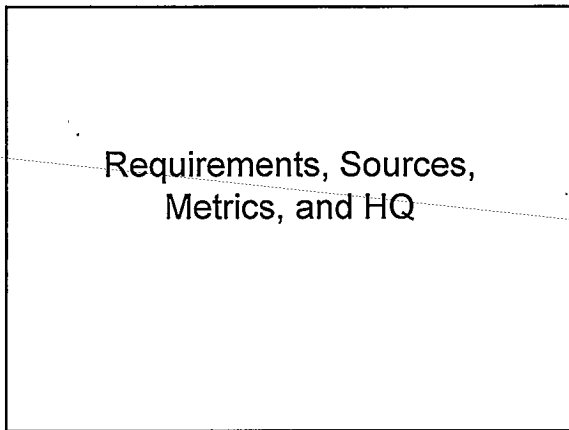
b7E

(S)



b1
b7E

(S)



Requirements, Sources,
Metrics, and HQ



b1
b7E

(S)



b1
b6
b7C
b7E

X

(S)

Click the Req. Number to view the collection requirement		
Req. Number	Title	EXPIRATION DATE
1		0810
2		0810
3		0810
4		0810
5		0810
6		0810
7		0810
8		0810
9		0810
10		0810
11		0810
12		0810
13		0810
14		0810

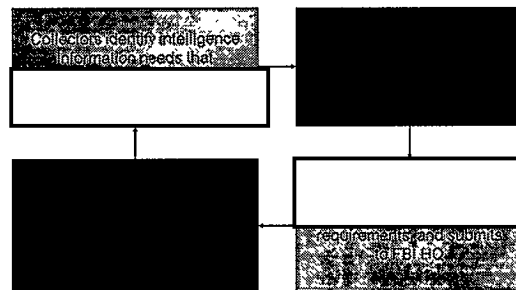
Counterproliferation Requirements



b1
b7D
b7E

Requirement Number	Requirement Title	Expiration Date
1		August 2007
2		July 2007
3		July 2007
4		January 2009
5		April 2008
6		October 2008
7		July 2007
8		June 2007
9		June 2008
10		June 2008
11		March 2007
12		April 2008
13		August 2007
14		November 2008
15		July 2008
16		August 2008
17		September 2007
18		May 2007
19		March 2007
20		March 2007
21		September 2007
22		July 2007
23		July 2008
24		June 2008

FBI Intelligence Cycle



b7D
b7E

Questions or Comments?

X

~~SECRET~~

(S)

CI Program Strategy 2007

FBI Strategic Focus:

ACTIVITIES RESULTS

(S)

FBI FCI Threat Matrix 2008 –

b1
b7D
b7E

(S)

(S)

[Redacted]

2008 Threat-Based & Issue-Driven Focus:
 Limited Resources Means Investigations & Operations
 Prioritized Against-

Prevent	-	WMD Proliferation
Prevent	-	Espionage
Prevent	-	CNA Compromise
Enhance	-	[Redacted]

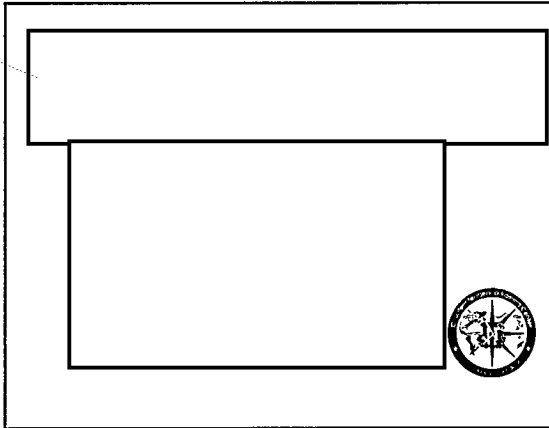
b1
b7E

~~SECRET~~

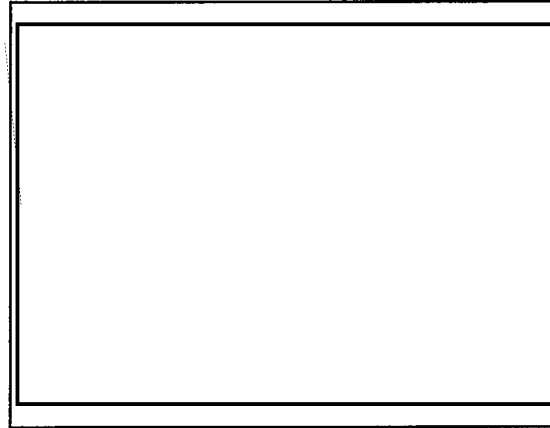
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



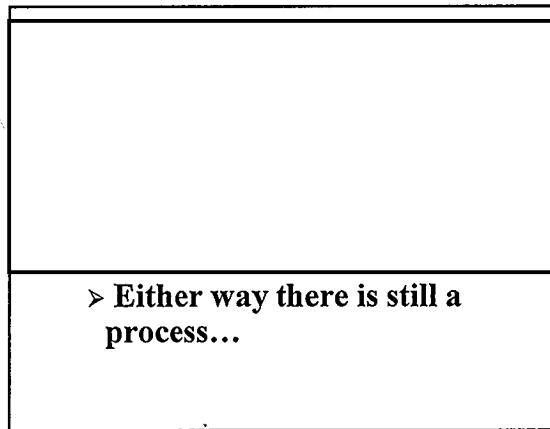
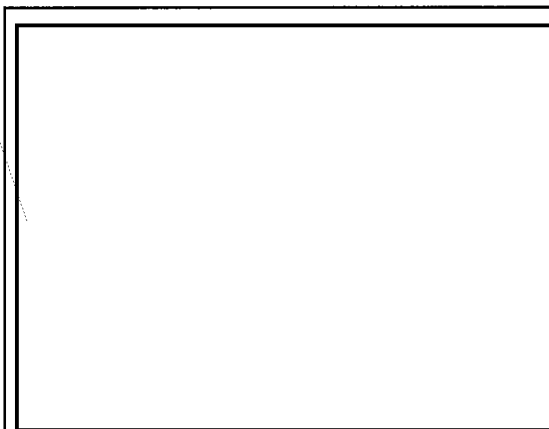
(S)



b1
b6
b7C
b7D
b7E

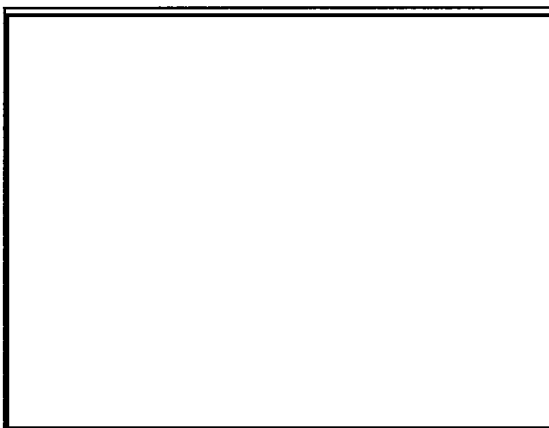
(S)

(S)



b1
b7E

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

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

ENGAGE IN STRATEGIC
PARTNERSHIPS

ENGAGE IN STRATEGIC
PARTNERSHIPS

INTERNAL PARTNERS

Proactive relationships with other FBI
Divisions

Regional / Joint Operations

Regional / Joint Threat Assessments

ENGAGE IN STRATEGIC
PARTNERSHIPS

RCIWG



ENGAGE IN STRATEGIC
PARTNERSHIPS

PARTNERSHIPS



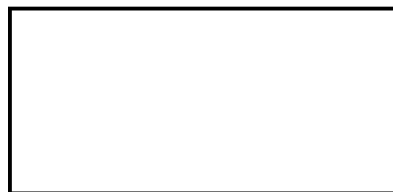
(S)

b1
b7E

ENGAGE IN STRATEGIC
PARTNERSHIPS
COUNTER INTELLIGENCE WORKING
GROUPS (CIWG)



ENGAGE IN STRATEGIC
PARTNERSHIPS
COUNTER INTELLIGENCE WORKING
GROUPS (CIWG)



b7E

~~SECRET~~

~~SECRET~~

7/13/2011

ENGAGE IN STRATEGIC
PARTNERSHIPS

(S)

b1
b7E

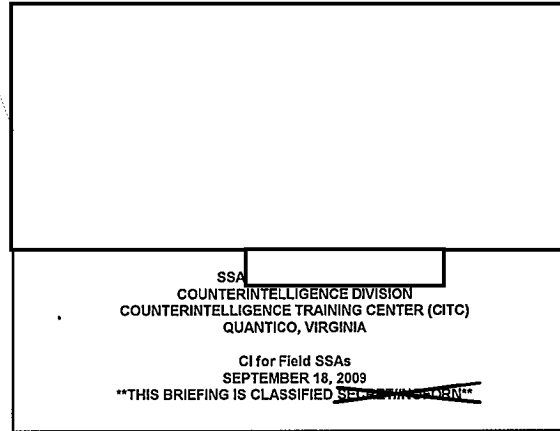
~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

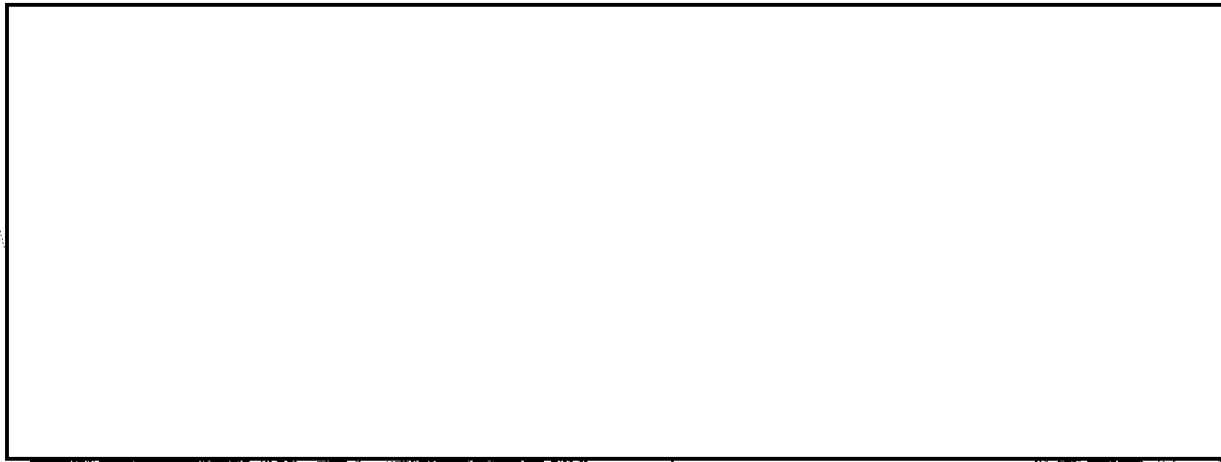
(S)



b1
b6
b7C
b7D
b7E

SSA [REDACTED]
COUNTERINTELLIGENCE DIVISION
COUNTERINTELLIGENCE TRAINING CENTER (CITC)
QUANTICO, VIRGINIA
CI for Field SSAs
SEPTEMBER 18, 2009
THIS BRIEFING IS CLASSIFIED ~~SECRET~~ UNCLASSIFIED

(S)



b1
b7D
b7E

(S)



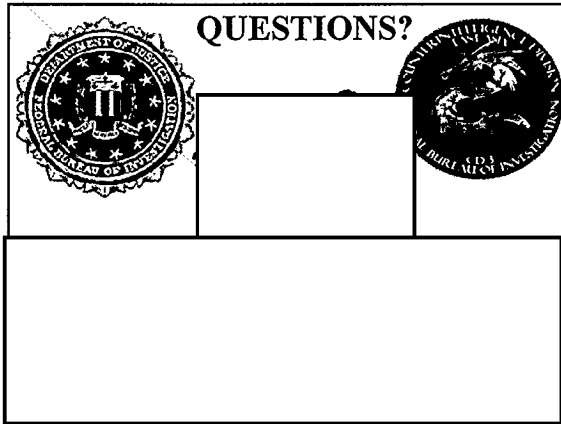
b1
b7D
b7E

~~SECRET~~

ACLURM043189

~~SECRET~~

(S)



(S)

b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

DECLASSIFIED BY 65179 DMH/STW
ON 03-01-2012

COUNTERINTELLIGENCE DIVISION
SPECIAL AGENT
CAREER PATH PROGRAM



CI SSA COURSE / NVRA
SEPTEMBER 14, 2009

uc

~~Origins of the program~~

The 9/11 Commission (7/22/2004)

"Adding a new domestic intelligence agency will not solve America's problems in collecting and analyzing intelligence within the United States. We do not recommend creating one. We propose ... a **specialized and integrated national security workforce at the FBI**, consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained, rewarded, and retained to ensure the development of an institutional culture imbued with a deep expertise in intelligence and national security."

b6
b7C

~~Origins of the program~~

Presidential Memo to the A.G. (11/23/2004)

"...Create within the FBI a specialized, integrated intelligence cadre (including special agents, analysts, linguists, and surveillance specialists), and implement a separate career track program permitting employees within the intelligence cadre to pursue their entire career... This effort shall include the establishment of specific requirements for training, career development, certification, recruiting, hiring and selection, and integration of the cadre into the FBI's field intelligence groups."

~~Origins of the program~~

Intelligence Reform Act of 2004 (12/17/2004)

"The Director of the Federal Bureau of Investigation shall develop and maintain a specialized and integrated national intelligence workforce consisting of agents, analysts, linguists, and surveillance specialists who are recruited, trained and rewarded in a manner which ensures the existence ... [of] an institutional culture with substantial expertise in, and commitment to, the intelligence mission of the Bureau."

~~Origins of the program~~

The WMD Commission (03/31/2005)

"The FBI's hybrid nature is one of its strengths. In today's world of transnational threats, the line between 'criminal activity' and 'national security information' is increasingly blurred... We believe it is critical that the National Security Service remain within the FBI. Personnel in the service would take advantage of its specialized career options, but agents in the service would go through law enforcement training along with their counterparts in the FBI's criminal divisions. Agents could laterally transfer between the service and the FBI's other divisions mid-career."

~~SACPP mission~~

The mission: Build more highly skilled agents + increase Intel capability

How: Through structured developmental opportunities:

- courses (Tracked via Virtual Academy) (Not Really)
- job experiences
- mentoring (ad hoc)
- documents
- presentations
- proficiency
- certifications

Linked to competencies developed in two separate studies

Who: Began designations [redacted]
Pilot offices began early 2007
May 7, 2007 EC From Director to All Field Offices
All field agents designated by September 2007

b7E

~~SECRET~~

the process - new agents

Current Process: Upon acceptance letter, ranks preferences and bio sheet prepared for each class
- selection is based on:

Stage 1 -

Stage 2 -

- components:

the process - new agents

Stage 3 -

- rotational transfer to large office
- continue following developmental plan

Stage 4 -

Stage 5 -

b7E

Special Agent Career Paths Recruiting and Hiring / Career Path Stages

■ = NSB ■ = Intel

Recruiting Hiring

Stage One
New Agent Training

Stage Two Stage Three Stage Four

Pre-designated at hire

* Tracked for developmental purposes, not a career path.

Initiative - SA Career Path Development and Training

Initiative Goal and Rationale

- The goal of this initiative is to build Special Agent career path plans. Each of the six career paths will have a customized plan of required training and experiences that individuals in that career path must complete to advance to the next stage of the career path. The strategic rationale is that by providing certain training and experiences at each stage of a Special Agent's career we will build a more proficient and knowledgeable Special Agent workforce in each career path.

Initiative Update

- All Special Agents are designated into one of six career paths
- The competencies for the stages of each career path have been determined.
- The development plans (i.e., training and experiential requirements for each stage of a career path) have been completed.
- Stage Two Field Skills Training courses for each of the career paths have been developed and training is on-going.

Stage One
New Agent Training

Stage Two Stage Three Stage Four

UNCLAS//SI//NF//FOUO Updated w/August data

b7E

SA Career Path Development and Training

- After NAT, the first training component of each career path is Field Skills Training. Field Skills Training is multiple-week, classroom-based training tailored to each career path.
- Stage 2 Field Skills Training classes for each career path have been developed.

Career Path Stage 2 Field Skills Training

UNCLAS//SI//NF//FOUO Updated w/August data

Background: Special Agents by Career Path Stage

Career Path	Stage Two	Stage Three	Stage Four	Total Agents in Career Path

Special Agents are currently in Stage Two of the SA Career Path

Notes:

- Stages of career path match GS-level progression for all career paths but Counterintelligence. Counterintelligence does not consider an agent to be in Stage Three of the career path until they have
- Total agents in career path includes all SAs with a designated career path, including all graduates of New Agents Training

UNCLAS//SI//NF//FOUO Updated w/August data

b7E

Initiative - SA Career Path Development and Training:
Counterintelligence Stage Two Field Skills Training

X

Counterintelligence (CI) Developmental Plan Revised 6/18/2008

Stage One	Stage Two	Stage Three	Stage Four

b7E

Counterintelligence Career Path Revised 6/18/2008
Stage Two - [Redacted]

Requirements:

Training [Redacted]

On-the-Job [Redacted]

Recommended:

Training [Redacted]

Other Developmental Opportunities [Redacted]

CITC Advanced Course List

- CI Espionage [Redacted]
- CI [Redacted]
- CI [Redacted]
- CI Surveillance [Redacted]
- CI [Redacted]
- CI Interview and Interrogation
- Counterproliferation for Investigators
- CI Technical Capabilities and Applications
- CI Domain Operations
- CI Lessons Learned

Counterintelligence Career Path Revised 6/18/2008
Stage Three - [Redacted]

Requirements:

Training [Redacted] An SA is considered CI proficient after completing [Redacted]

On-the-Job [Redacted]

Recommended:

Training [Redacted]

Other Developmental Opportunities [Redacted]

CITC Advanced Course List

- CI Espionage [Redacted]
- CI [Redacted]
- CI [Redacted]
- CI Surveillance [Redacted]
- CI [Redacted]
- CI Interview and Interrogation
- Counterproliferation for Investigators
- CI Technical Capabilities and Applications
- CI Domain Operations
- CI Lessons Learned

*A CD specific conference of 3 days or more may be substituted for one advanced course

b7E

7/13/2011

DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012

b6
b7C
b7E

Counterespionage	
Organization & Operations	
Created by: [redacted] Version: 1.0/0.0	

Counterespionage	
	Introduction

Counterespionage	
	Introduction

~~SECRET~~

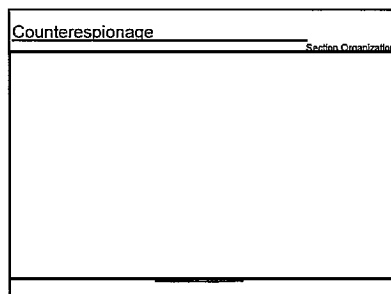
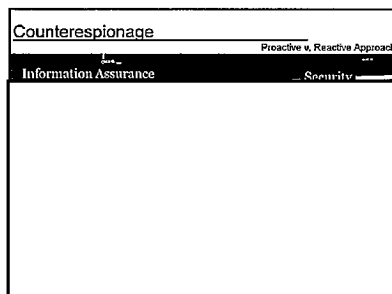
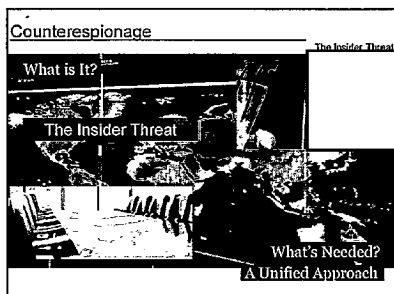
~~SECRET~~

b6
b7C

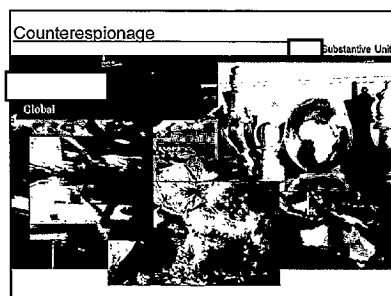
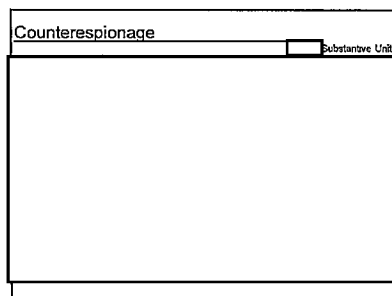
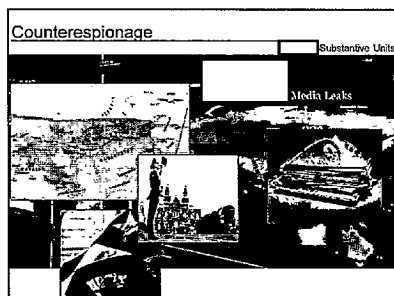
Counterespionage	
Federal Espionage Statutes	
	
Title 18 USC 793 - Gathering, Transmitting, or Losing Defense Information	
Title 18 USC 794 - Gathering or Delivering Defense Information to Aid a Foreign Government	
Title 18 USC 798 - Disclosure of Classified Information	
Title 18 USC 1831 - Economic Espionage	
Title 18 USC 1832 - Theft of Trade Secrets	
Title 18 USC 1924 - Unauthorized Removal & Retention of Classified Documents or Materials	
Title 22 USC 611a - Agents of Foreign Governments (FAMA)	
Title 50 USC 1701 - International Emergency Economic Powers Act	
Title 50 USC 782 - Internal Security Act of 1950	

Counterespionage	
Espionage Cases Originale From	

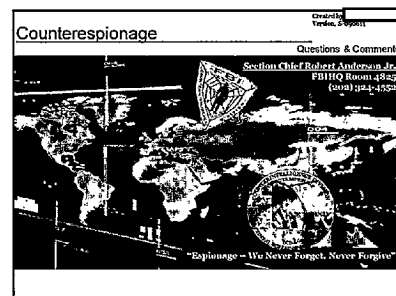
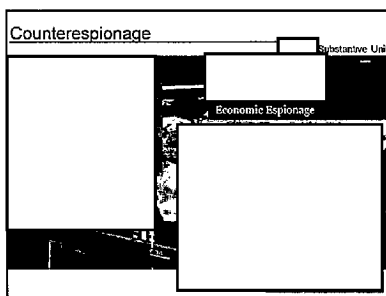
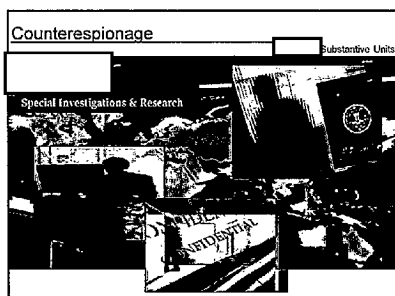
Counterespionage	
All Referrals	



b6
b7C
b7E



b7E



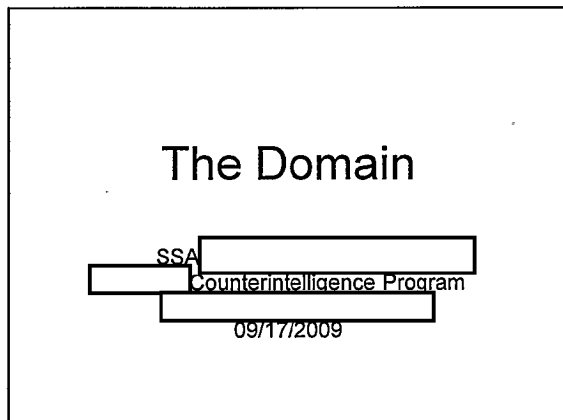
b6
b7C
b7E

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

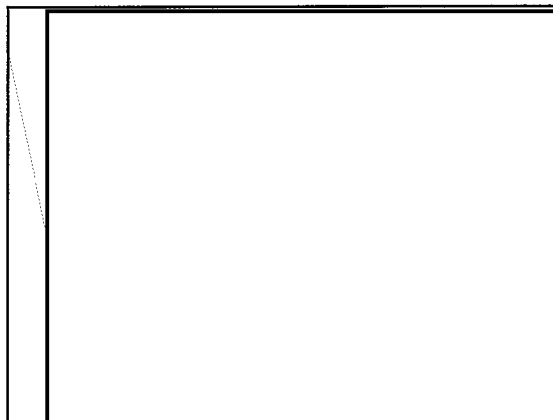
7/13/2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

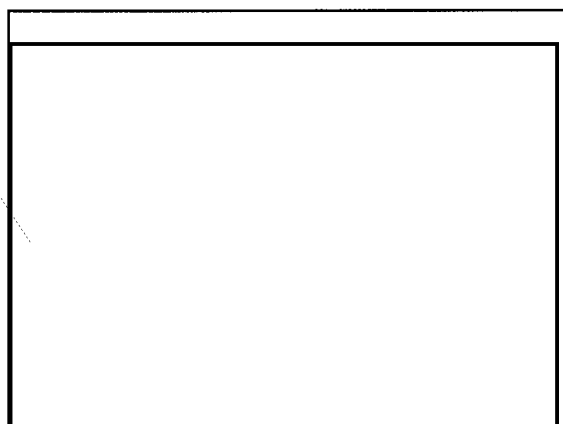


(S)



b1
b6
b7C
b7E

(S)



b1
b7E

~~SECRET~~

7/13/2011

~~SECRET~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

This presentation is classified ~~SECRET~~.
Information from this presentation should not be
disseminated outside the FBI without prior
FBIHQ approval.

Goals and Objectives

To familiarize personnel with:

~~SECRET~~

b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

HELP! Where do I go?

~~SECRET~~

Why did this happen?

- Key inhibitors of old policies were administrative, not operational.
- Fragmented programs having conflicting policies and data rule sets not designed for information sharing.

~~SECRET~~

b1
b7E

Streamlining Procedures

~~SECRET~~

Streamlining Procedures

~~SECRET~~

(S)

~~SECRET~~

ACLURM043198

~~SECRET~~

7/13/2011

Streamlining Procedures

- Executives in the Field are capable of making many decisions currently reserved for HQ.

- Disclosure of [redacted]
[redacted]

(S)

~~SECRET~~

Streamlining Procedures

No more CDC review of serials [redacted]
[redacted]

No more SSA 60 day file reviews [redacted]
[redacted]

No alternate case agent needed (only a co-case agent [redacted]).

b1
b7E

~~SECRET~~

Admonishments

- Provided to [redacted] within 90 days of opening or before first tasking:
[redacted]

- Others if they apply (Section 4)
- Provided every year

(S)

~~SECRET~~

Approval Authorities to Lowest Levels Where Possible

- Approvals, Authorities, and Delegation
 - Unless specified otherwise in the manual, all approval authorities may be delegated [redacted]
 - Approval authorities may be provided by [redacted]
 - (See approvals worksheet in each Field Office)

b1
b7E

~~SECRET~~

Some old rules still apply...

- [redacted]
- [redacted]

~~SECRET~~

(S)

Some old rules still apply...

[redacted]
[redacted]
[redacted]

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

7/13/2011

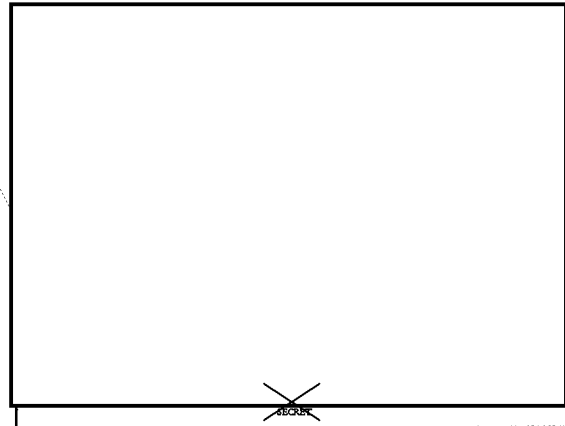
(S)

Some old rules still apply...



- Buckley Amendment

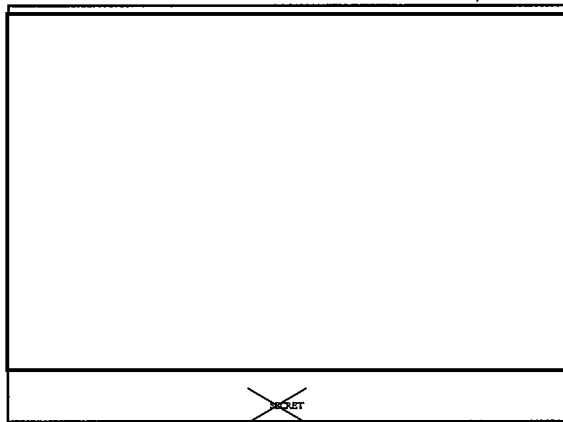
~~SECRET~~



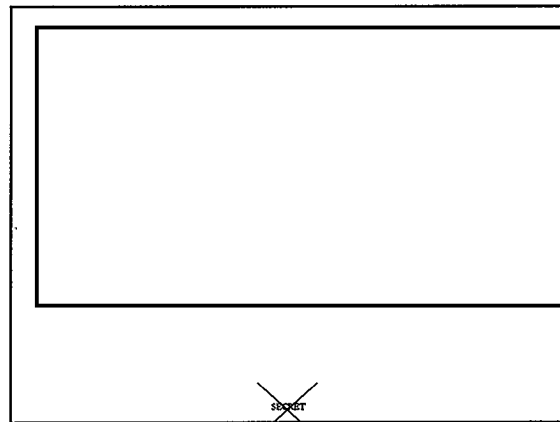
~~SECRET~~

b1
b7E

(S)



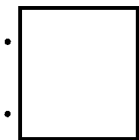
~~SECRET~~



~~SECRET~~

b1
b7E

Reporting



- EC if going out of Field Office



~~SECRET~~

Additional Training Issues

- Classification
 - See new classification guidelines
- Other issues

~~SECRET~~

b7E

~~SECRET~~

~~SECRET~~

7/13/2011

OIG Review of FBI Handling and Oversight of [REDACTED] Unclassified Executive Summary

FBI's [REDACTED] CI Program
• Low priority • Focus on [REDACTED] Cold War • Overwhelmed by volume • Understaffed/overworked/regular turnover in management • Authority delegated to Field
~~SECRET~~

b6
b7C
b7D
b7E

• College grad [REDACTED] • EOD October [REDACTED] • FOA - [REDACTED] • Started working [REDACTED] • [REDACTED] SSAs relied on judgment and recommendations • [REDACTED] SSA of [REDACTED]
~~SECRET~~

• [REDACTED] emigrated to U.S. • [REDACTED] graduated High School [REDACTED] • [REDACTED] • [REDACTED] student developed contacts with persons of interest to FBI • [REDACTED]
~~SECRET~~

b6
b7C

Predication for [REDACTED]
• Lives in building characterized as [REDACTED] • General Manager - [REDACTED] • [REDACTED] • Relationship with [REDACTED] • [REDACTED] FBI closed case
~~SECRET~~

Objective of [REDACTED]
• Determine if threat to National Security • Determine willingness to cooperate
~~SECRET~~

b6
b7C

~~SECRET~~

~~SECRET~~

7/13/2011

OIG Finding

- Case assigned to inexperienced agent admittedly not interested in FCI
- Closed case without interview indicating can not interview subject of investigation
- Lost opportunity to fill intelligence gap on [redacted] request for technology

~~SECRET~~

Phase I

- August 1982 - [redacted] re-opens investigation and interviews
- After several interviews [redacted]

[redacted] affair starts

b6
b7C
b7D
b7E

~~SECRET~~

Phase II

- Limited supervision [redacted]
- [redacted] becomes U.S. Citizen - [redacted]
- FBI Plan - have [redacted]
 - Encouraged to flaunt contacts with FBI
 - Encouraged to flaunt high-profile status in [redacted] community

~~SECRET~~

Phase II

~~SECRET~~

b6
b7C
b7D
b7E

Phase II

[redacted] provided positive feedback on reporting

- Affair with [redacted] started

~~SECRET~~

Phase III

- Meeting at HQ agreed to continue operations - issues not fully disclosed
- FBIHQ decides to let [redacted] handle situation but failed to follow up

~~SECRET~~

b6
b7C
b7D
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

Phase III

[redacted]
[redacted]
[redacted] FBIHQ SSA requests FBIHQ Analyst to
[redacted] based on issues [redacted]

~~SECRET~~

Phase IV

[redacted] promoted to SSA
- Keeps handling [redacted]
• ASAC permits [redacted] to sign out own paper
[redacted] - Espionage case opens on
squad
[redacted] ASAC requests [redacted] renew two agent
exemption
[redacted] FBI receives information on [redacted]

~~SECRET~~

b6
b7C
b7D
b7E

Retires

- [redacted]
[redacted]
- Assumes will be investigated
 - Did not tell [redacted] of possible investigation
- [redacted]

~~SECRET~~

Investigation

[redacted] - FBIHQ uncovers original [redacted]
reporting
[redacted] investigation begins
[redacted]
• 9-11-2001 delays investigation

~~SECRET~~

b6
b7C
b7D
b7E

Investigation

[redacted] - special techniques authorized
shows sexual relationship
[redacted]

~~SECRET~~

Aftermath

[redacted] to every FO
[redacted] process implemented
• FBIHQ oversight of [redacted]
• FBIHQ [redacted] Units created

~~SECRET~~

b6
b7C
b7D
b7E

~~SECRET~~

Conclusion

- **OIG Recommendations**
 - Continue new [redacted] process
 - Commit appropriate resources to [redacted]
 - New subsection in [redacted]
 - [redacted]
 - Thorough periodic reinvestigations [redacted]
 - [redacted]

~~SECRET~~

Conclusion

- **OIG Recommendations**
 - Maintaining records of documents passed to and conversations [redacted]
 - Alternate case agents [redacted]
 - Limited time agent can [redacted]
 - [redacted]
 - Prohibiting blanket exemptions to rules

~~SECRET~~

b7E

(S)

(S)

[redacted]

~~SECRET~~

[redacted]

~~SECRET~~

b1
b7E

[redacted] **Milestones**

- **Initial Opening Communication**
- **Continuously** [redacted]
- [redacted]

~~SECRET~~

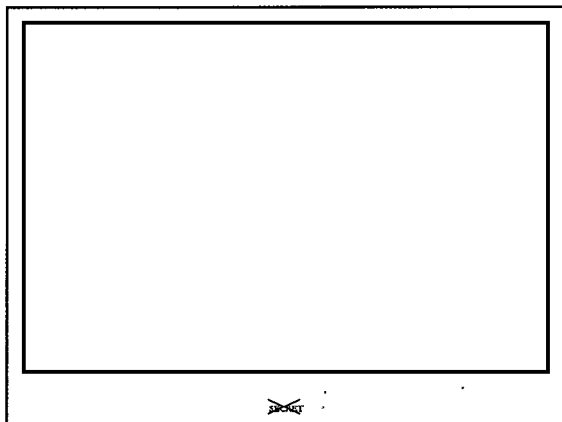
Changes/Issues
Types of [redacted] Reviews

- Primary
- Secondary
- Enhanced

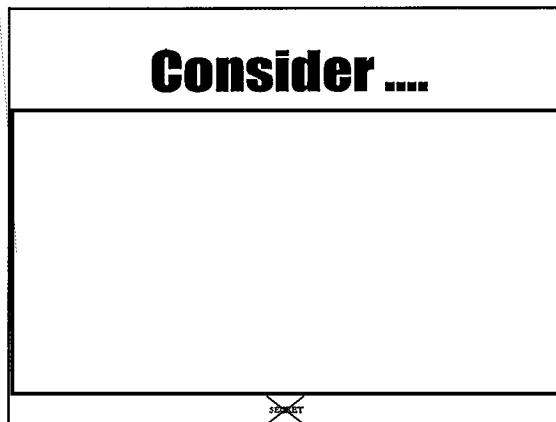
Done at FBIHQ

~~SECRET~~

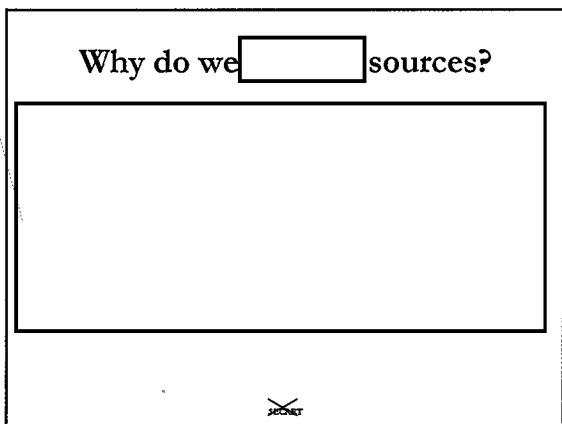
b7E



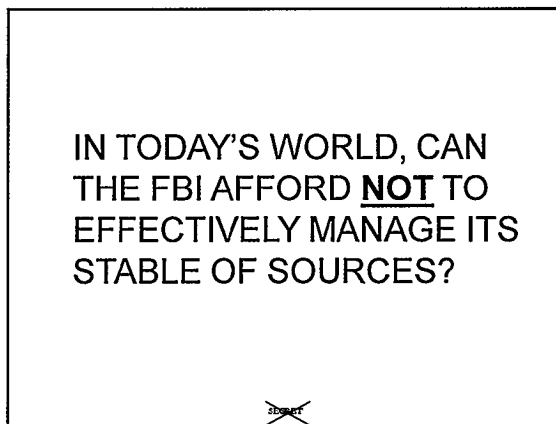
(S)



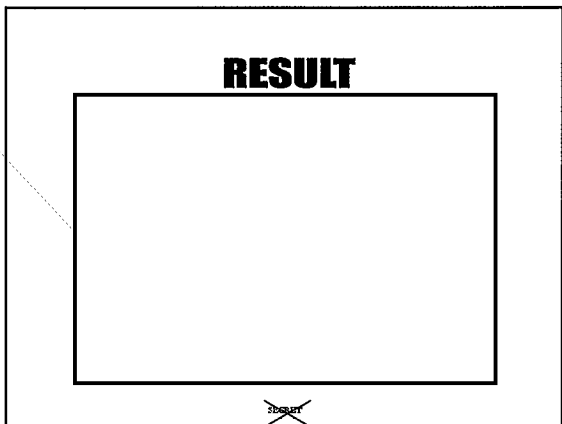
b1
b7E



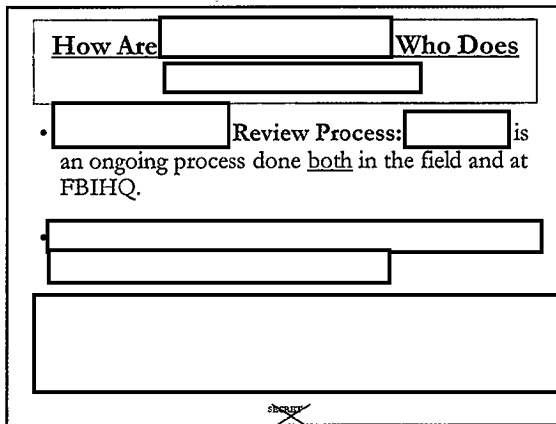
(S)



b1
b7E



(S)

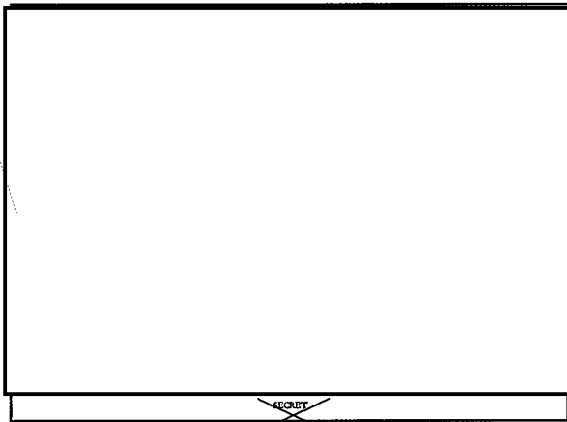


b1
b7E

~~SECRET~~

7/13/2011

(S)



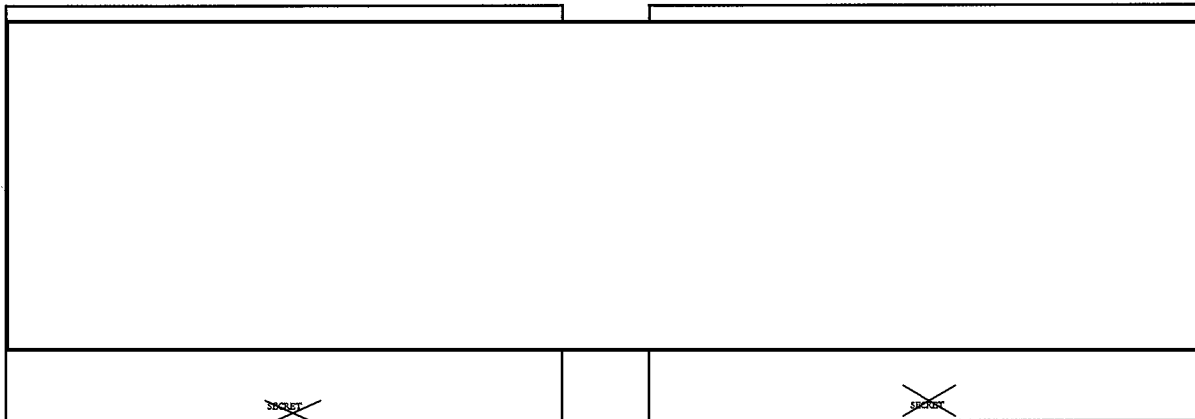
IN THE BROADER CONTEXT...

-Are we receiving good return on investments of time and money?
-Are we contributing to overall USIC requirements?

-Problems being uncovered?

b1
b7E

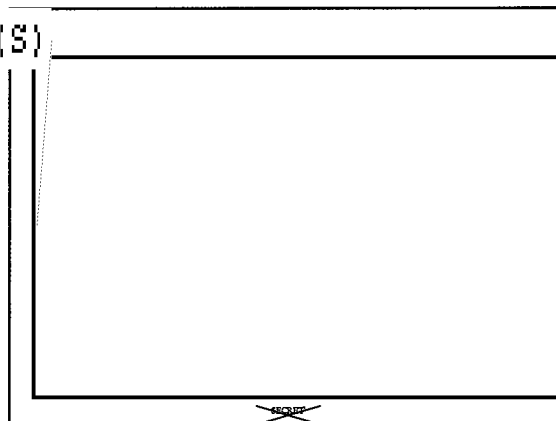
(S)



b1
b7E

What can the Field Office do to support the effort?

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

(S)

Process

•

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

DO YOU...

- Maintain objectivity
- Ask how this source is contributing to

~~SECRET~~

(S)

Steps can take now

-Compliance issues:

-Travel concurrence

-Routing communications: PLEASE send

~~SECRET~~

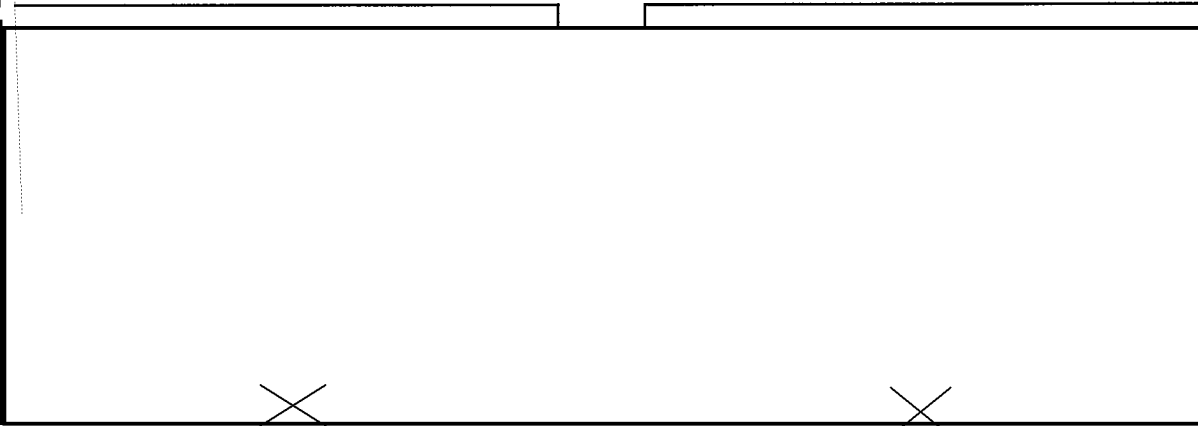
b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

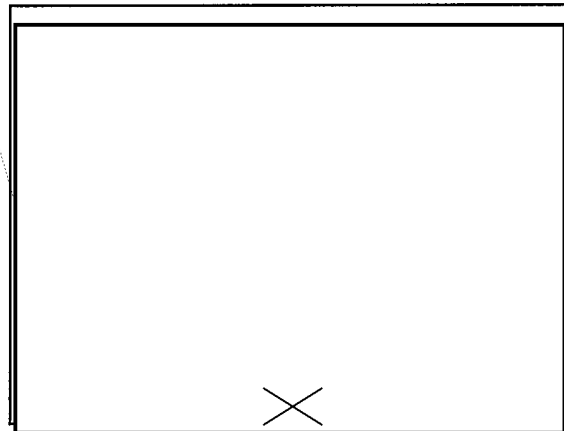
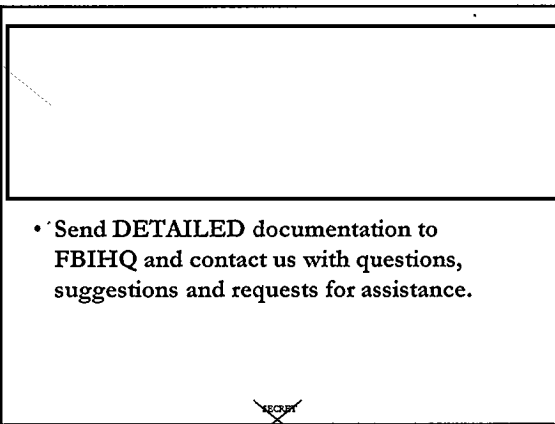
(S)



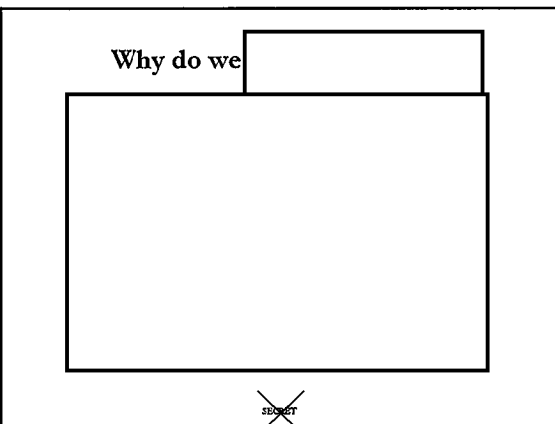
b1
b7E

(S)

(S)



b1
b7E



b6
b7C
b7E

~~SECRET~~

~~SECRET~~
(when filled out)

DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012

Counterintelligence Squad Summary

Office:

FSL/TSL:

Day 1 Priorities

- 1) What are your priorities:
 - a.
 - b.
 - c.
- 2) Describe the traditional threat in your area
 - a.
 - b.
 - c.
- 3) Describe the threat in your area
 - a.
 - b.
 - c.
- 4) Are your priorities in line with the national strategy? If not, explain:
- 5) Do your cases address your threat? If not, explain:

b7E

~~SECRET~~
(when filled out)
ACLURM043209

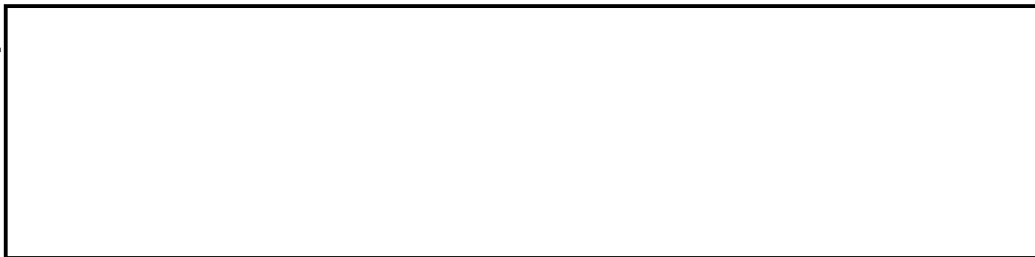
FBI042109

~~SECRET~~
(when filled out)

Day 2 CI Ops/Sources/Strategic Partners/Cross Program
Coordination

- 1) Does your CHS base support your priorities?
- 2) How well is your squad integrated into the
Intelligence Program?
 - a. Embedded IAs?
 - b. How do you disseminate intelligence to the FIG?
 - c. Do you and your Agents understand/know your
program requirements?

3)



b7E

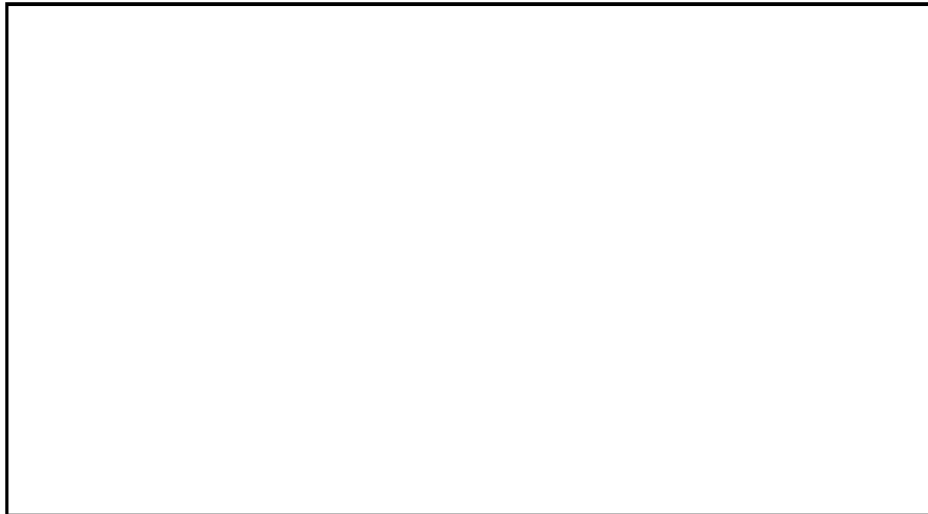
~~SECRET~~
(when filled out)
ACLURM043210

FBI042110

~~SECRET~~
(when filled out)



4) Who are your strategic partners?



b7E

5) Are you meeting regularly with your colleagues in the office from CT, CY and WMD and coordinating investigations when appropriate?

a. Do you know each other's basic investigative priorities?

~~SECRET~~
(when filled out)
ACLURM043211

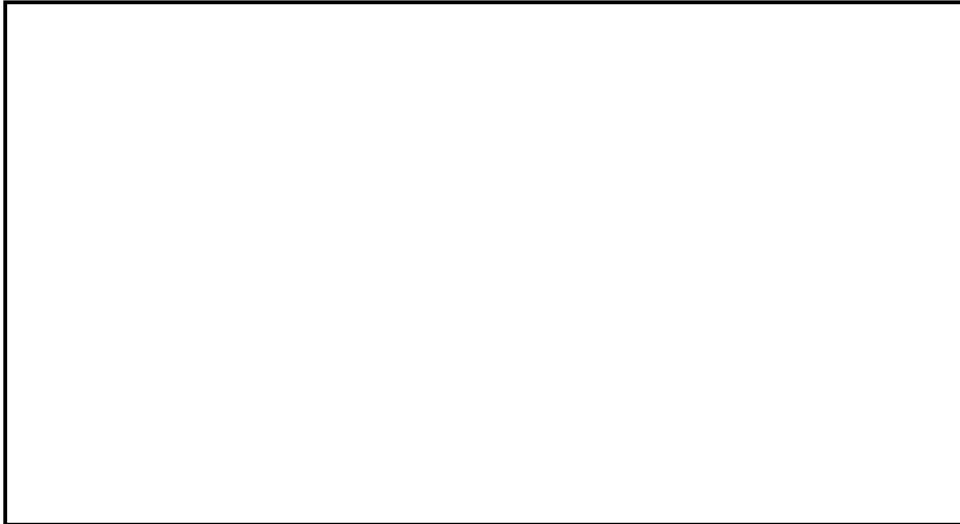
FBI042111

~~SECRET~~
(when filled out)

Day 3 Resources

- 1) Do you utilize investigative tools in your operations?

a. How much do you interact with those squads/coordinators?

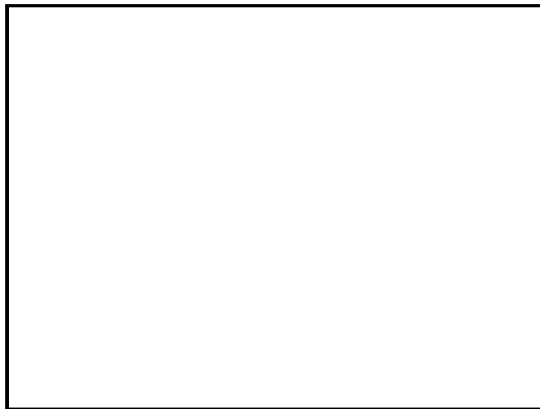


b7E

2)

Day 4 CI Domain

- 1) Describe your domain

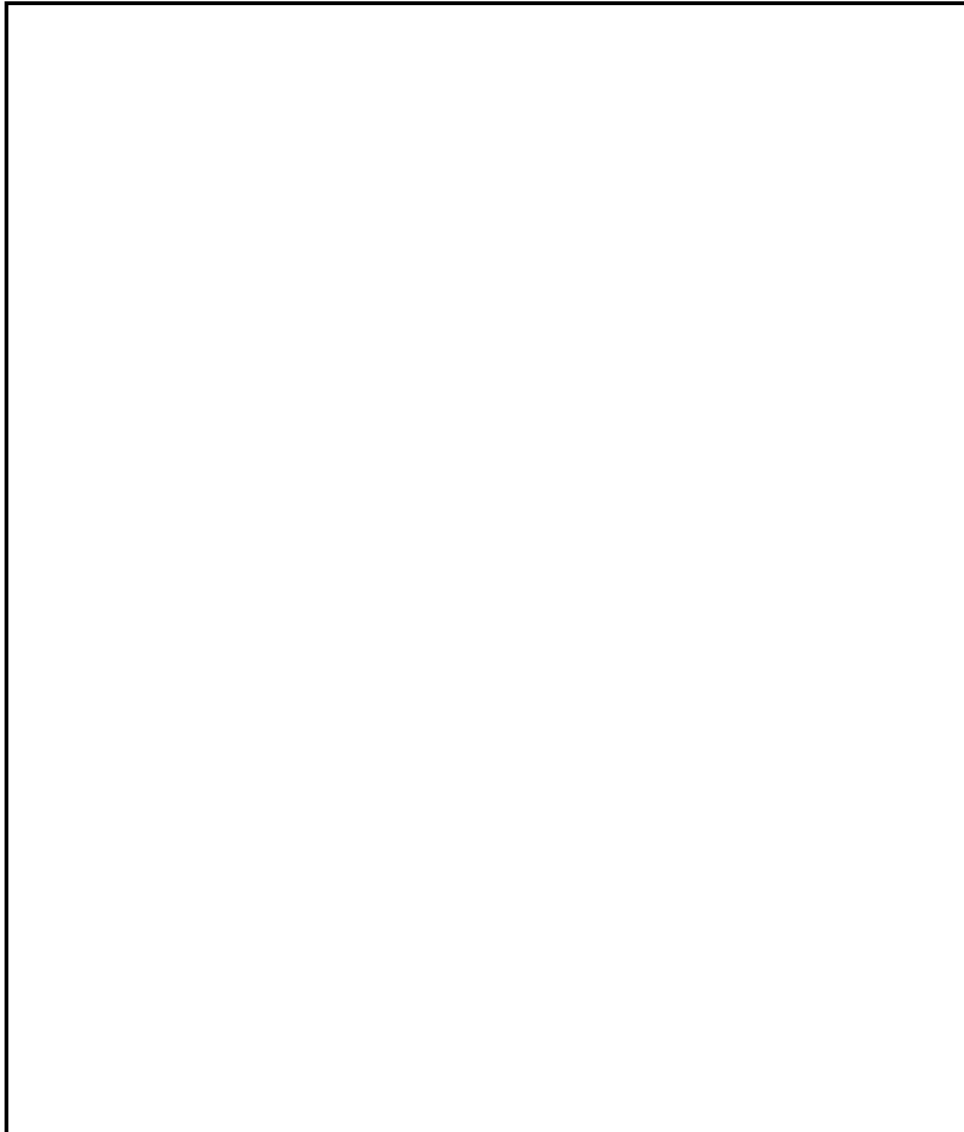


b7E

~~SECRET~~
(when filled out)
ACLURM043212

FBI042112

~~SECRET~~
(when filled out)



b7E

2) Are you aware of the issues in your domain?

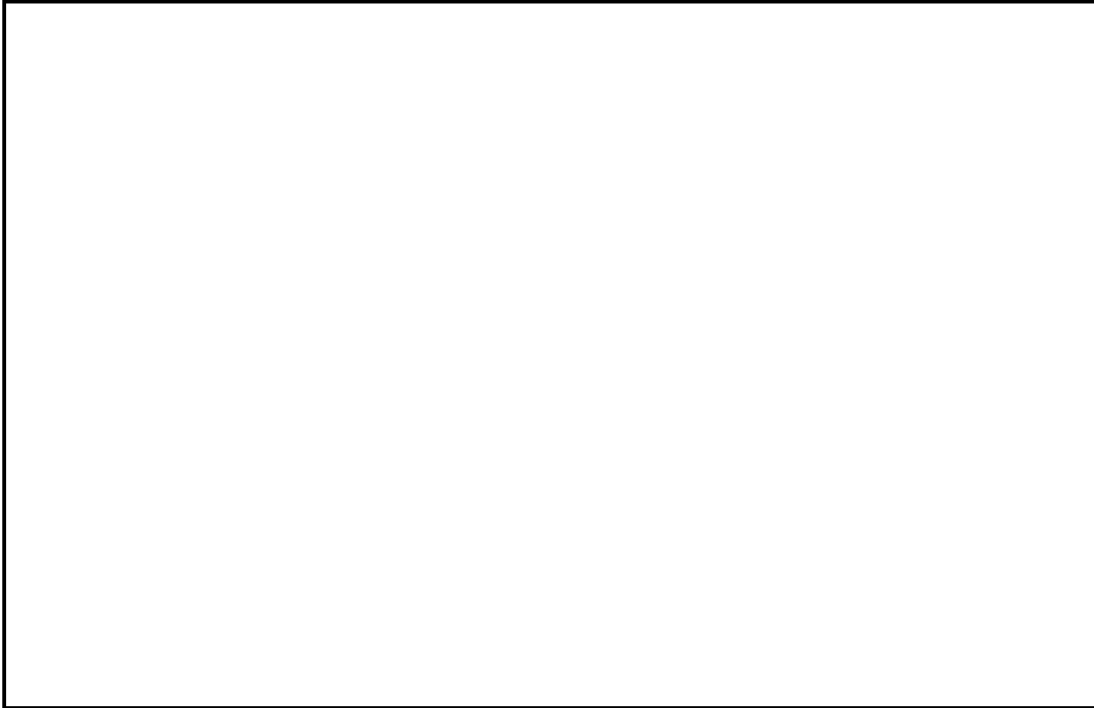
b7E

~~SECRET~~
(when filled out)
ACLURM043213

FBI042113

~~SECRET~~
(when filled out)

Day 5 Cyber



b7E

~~SECRET~~
(when filled out)
ACLURM043214

FBI042114

7/13/2011

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~



FEDERAL BUREAU OF INVESTIGATION



Counterintelligence Program
Strategic Resource and Performance Management

[Redacted Box]

17 September 2009
Prepared by CD Executive Staff

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Course Objectives

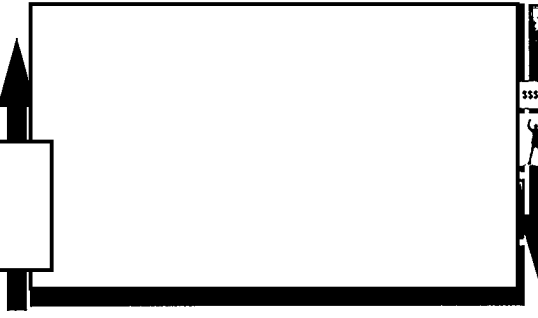
- Objective #1: Define the big picture and the cycle of [Redacted]
- Objective #2: [Redacted]
- Objective #3: SMS Measures and Objectives - [Redacted]
- Objective #4: Counterintelligence [Redacted]
- Objective #5: External Resource Decisions - [Redacted]
- Objective #6: COMPASS and Executive Level Reporting - [Redacted]
- Objective #7: Next Steps - [Redacted]

~~SECRET//NOFORN~~

b7E

~~SECRET//NOFORN~~

The Big Picture



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Counterintelligence

Strategic Priorities:

- Counterintelligence Division driven
- Program Managers manage by issues

[Redacted Box]

↕

COUNTERINTELLIGENCE CLASSIFICATIONS

↕

Strategy Management System (SMS):

- Director/Corporate driven
- Program Managers manage by objectives and accomplishments

[Redacted Box]

↕

Field Office

[Redacted Box]

~~SECRET//NOFORN~~

b7E

~~SECRET//NOFORN~~

CI Strategic Priorities

Issue Threat:

[Redacted Box]

Assumptions:

- Most/All priorities correlate [Redacted]
- Response to National Requirements
 - Other high [Redacted] topics
 - Other medium [Redacted] topics
- Operational Support to the IC

[Redacted Box]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Field Office Resource and Strategy Drivers

Strategy Performance Session (SPS):

- Field Office and HQ
- Performance Driven

[Redacted Box]

Resource Management Allocation (RMA):

- FO request additional Agent FSL or transfers

[Redacted Box]

[Redacted Box]

CI Field Office Reviews

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

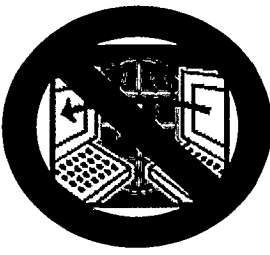
~~SECRET~~

7/13/2011

~~SECRET//NOFORN~~

Data Sources

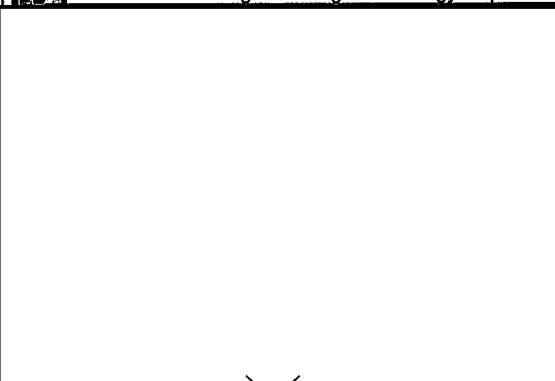
-
- Operational Support Programs
- COMPASS
 - Field Agent TURK
- Manual Records
 -



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Counterintelligence Program Strategy Map

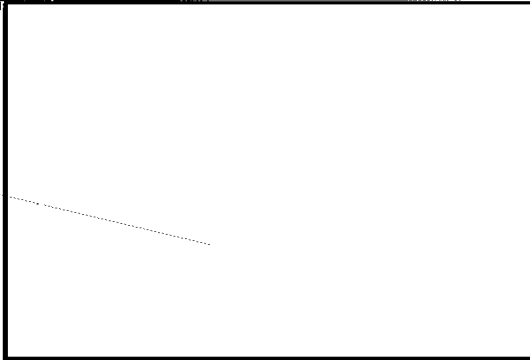


~~SECRET//NOFORN~~

b7E

~~SECRET//NOFORN~~

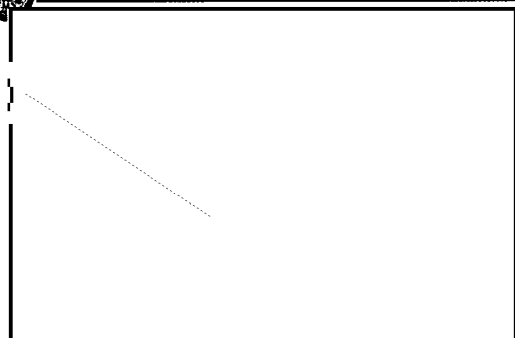
542 Stats Aligned to SMS Objectives



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

542 Stats Aligned to Inputs and Results



* SMS Objectives highlighted in red also appear in the CI Inspection Review

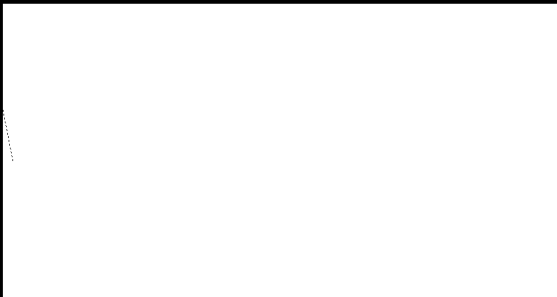
~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

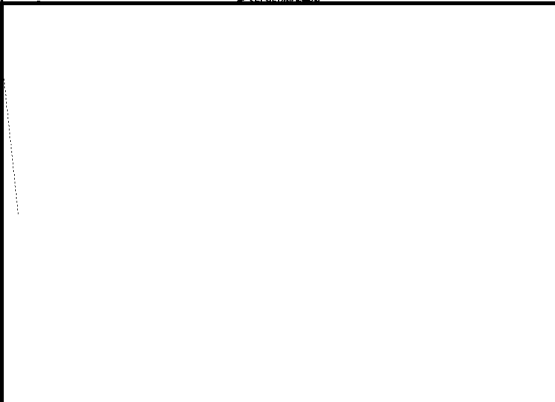
SMS and FD-542

Comparing Field Agent TURK and
FD-542 Statistical Accomplishments Aligned with SMS Objectives
All Field Offices
Mid-year FY 2009



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



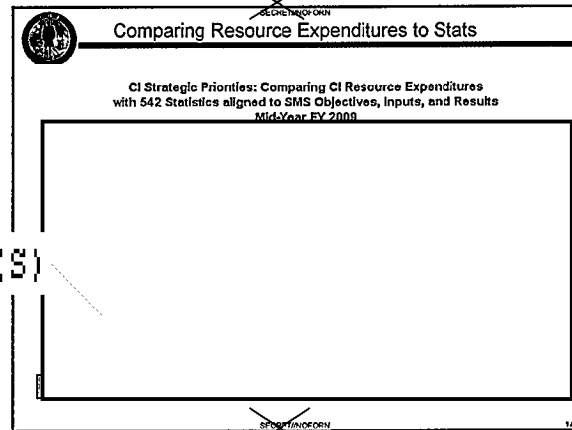
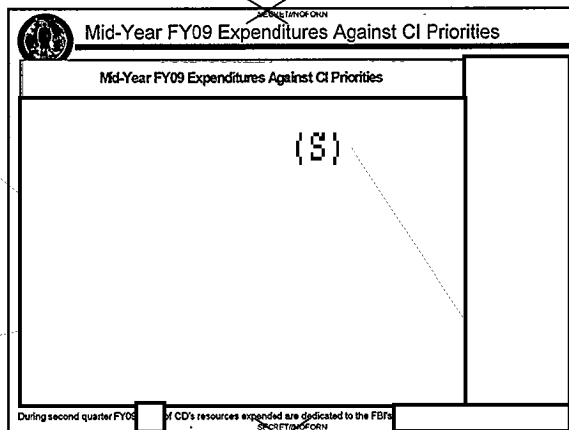
~~SECRET//NOFORN~~

b1
b7E

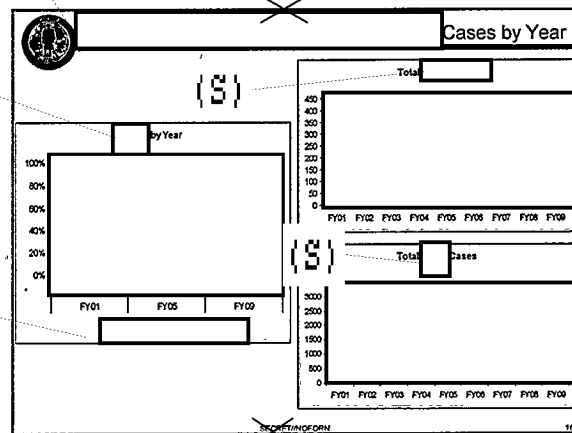
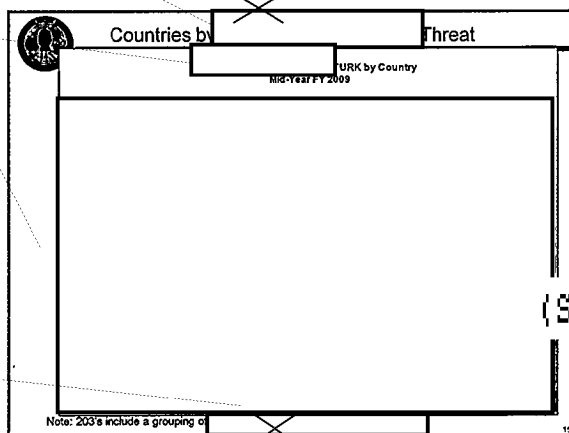
~~SECRET~~

~~SECRET~~

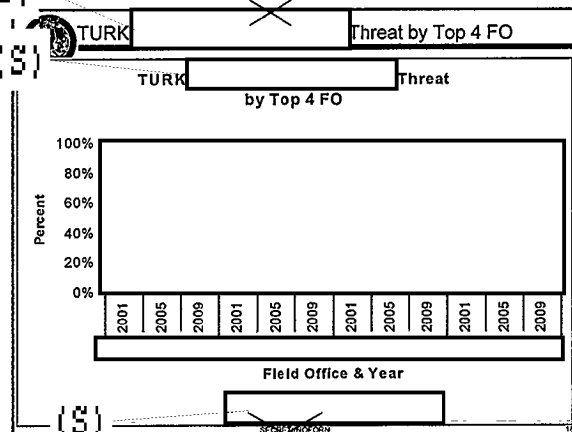
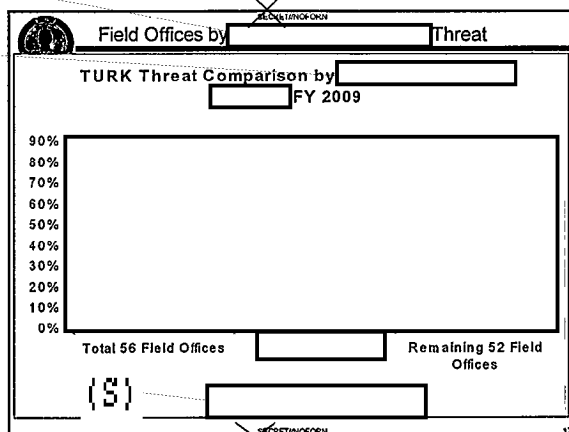
7/13/2011



b1
b7D
b7E



b1
b7D
b7E

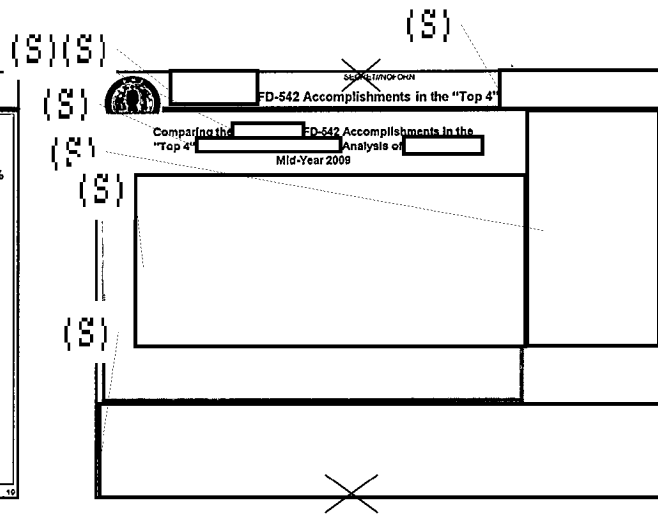
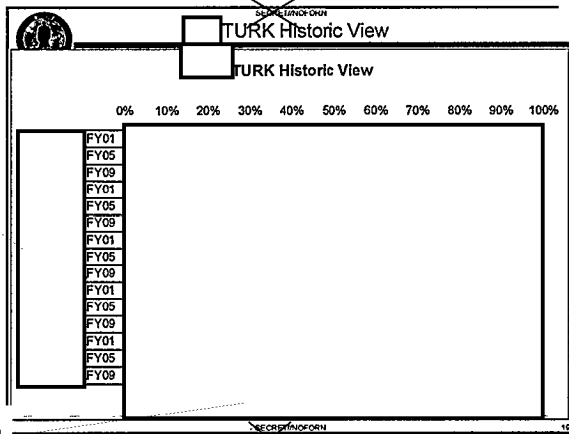


b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011



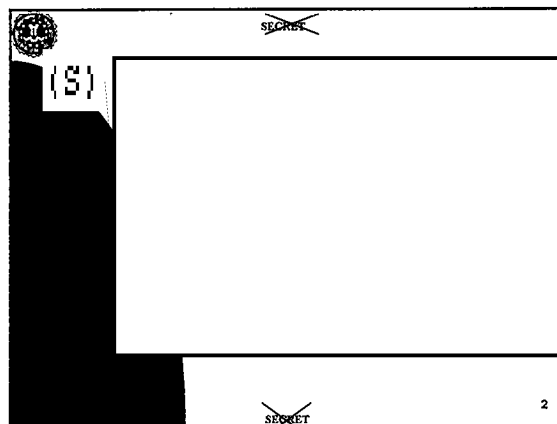
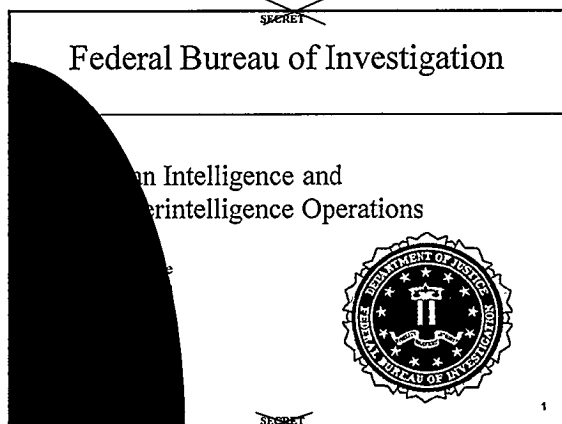
b1
b7D
b7E

~~SECRET~~

7/13/2011

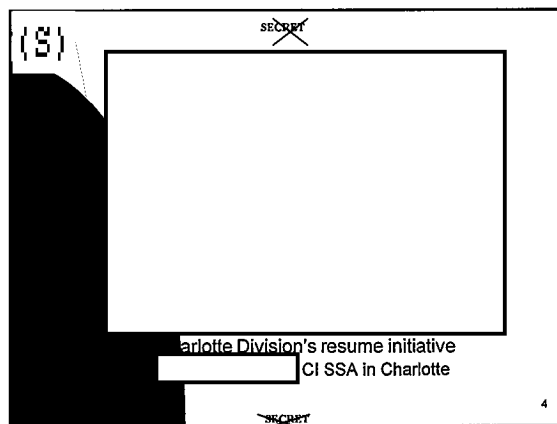
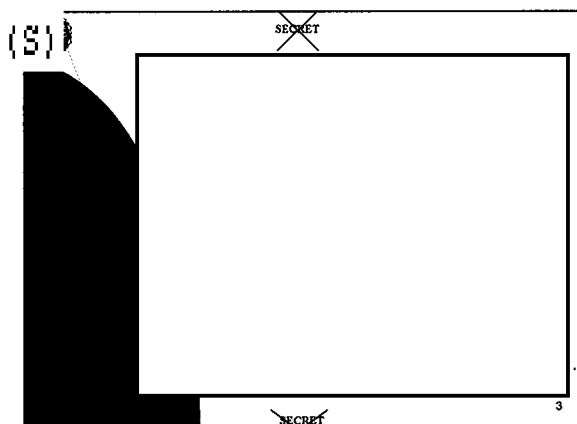
~~SECRET~~

DATE: 03-02-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 03-02-2037

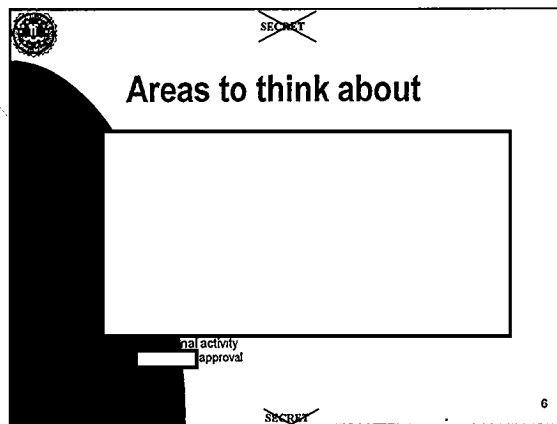
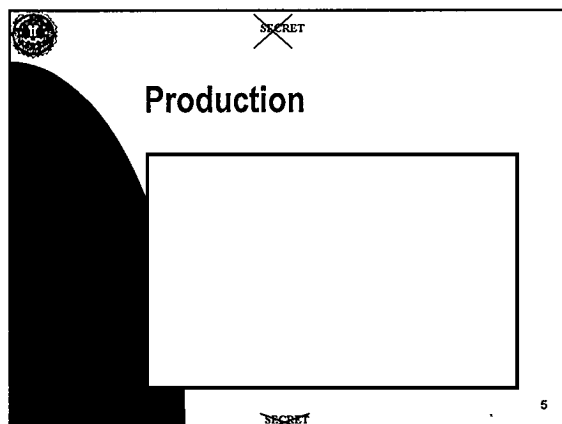


b1
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b1
b6
b7C
b7E



b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~//OC, NF

7/13/2011

~~SECRET~~

Summary

- Be very nice to your coordinator
- Encourage use of liaison contacts as part of intelligence base
 - ◆ No need to open everyone
- Keep on top of your asset files
 - ◆ File reviews
- Quality counts
-

~~SECRET~~

7

~~SECRET~~

Any questions?

~~SECRET~~

8

b7E

~~SECRET~~

~~SECRET~~

7/13/2011

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

~~SECRET~~

Federal Bureau of Investigation

Counterintelligence Operations



~~SECRET~~

1

~~SECRET~~

This briefing is intended to:

- Basic overview of CI ops from a SSA's perspective
 - ◆ Ops 101
 - ★ Priorities
 - ★ What to open
 - ★ Types of cases
 - ★ Pitfalls (just FYIs...)
 - ★ Admin issues
- Your input/experiences are welcome; please chime in

~~SECRET~~

2

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~

Counterintelligence Operations

Every FBI division's CI program will be different

- ◆ Threats
- ◆ Resources
- ◆ Experience level

What is important for a CI program?

Results: Lots of good cases, but what are we getting from them?

SAPR/SAC PAR

- ◆ It's not about the numbers, it's about the numbers
- ◆ Know what is required, but don't let it drive your cases

Determine what you do well, run with it.

~~SECRET~~

3

~~SECRET~~

Types of Investigations

- Assessment
 - ◆ "...authorized purpose.."
 - ◆ FD-71
 - ◆ 30-day reviews
 - ◆ Lead to case or close
- Preliminary Investigation
 - ◆ "...is or may be..."
- Full Investigation
 - ◆ "...articulable factual basis..."

~~SECRET~~

4

~~SECRET~~

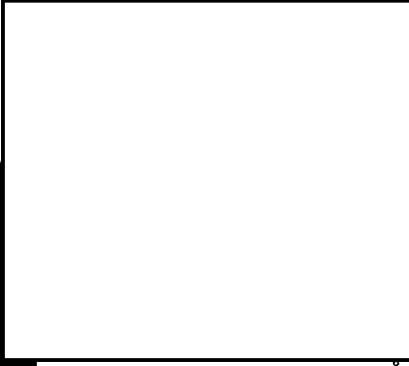
Authorities

- Refer to:
 - ◆ DIOG
 - ★ Watch those SIMs
 - ◆ CD Program Guide (supplement to DIOG)
 - ★ Specifics for reporting in CD matters
- Talk to the right people
 - ◆ CDC/NSLB
 - ◆ Auditor
 - ◆ UC Coordinator

~~SECRET~~

5

~~SECRET~~



~~SECRET~~

6

b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~//OC, NF

7/13/2011

(S)

~~SECRET~~

~~SECRET~~

- Others
- If your priorities do not match national ones, need to get HQ approval

~~SECRET~~

7

Issue threats

- Esionage
- Proliferation
- Economic Espionage
- Targeting [redacted]
- Covert influence
- Foreign intelligence activities

b1
b7D
b7E

(S)

What's the goal once a case is opened?

- Neutralization [redacted]
- Recruitment [redacted]
- Collection/analysis [redacted]
- Exploitation
 - Disinformation?
 - Work with USIC to exploit data

(S)

(S)

~~SECRET~~

9

Who can harm me?

- Things to consider:
 - Threat's [redacted]
 - Threat's capability [redacted]
- Any other USIC focused on threat? [redacted]

(S)

~~SECRET~~

10

b1
b7E

Case openings

- Does the case:
 - Fall within authorities of AG Guidelines
 - Meet a priority
 - Support the national strategy
 - Have some other reason why the case should be opened
 - Target of opportunity
 - Support to other agency or liaison service
- Help or harm
 - If they can help the USIC then identify, assess and talk to them
 - If they can harm the US then identify, investigate thoroughly and neutralize the threat
 - If they can neither help nor harm, no sense in opening a case
 - But, might someone else in the USIC be interested?

~~SECRET~~

11

Country threat investigation

- Traditional CI work
 - Establishments [redacted]
- Identify foreign power: [redacted]

(S)

(S)

(S)

~~SECRET~~

12

b1
b7D
b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~//OC, NF

7/13/2011

(S)

~~SECRET~~

Country threat cases



- * Approach or move on
- ♦ NFPO, NFPO, NFPO

~~SECRET~~

13

(S)

~~SECRET~~

Country threat cases, cont...



- ♦ Where's the priority? Intel or crim?
- ♦ Help or harm

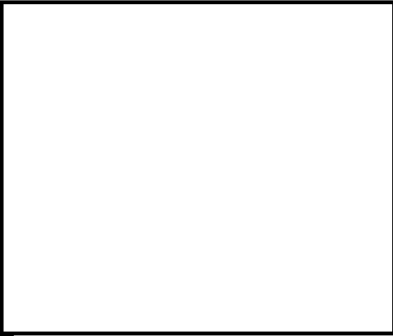
~~SECRET~~

14

b1
b7E

(S)

~~SECRET~~



~~SECRET~~

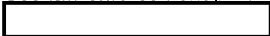
15

(S)

~~SECRET~~

cont...

- Use law enforcement partners



- * Lead information
- * Access to information/databases
- * Admin subpoena is very helpful
- * More familiar with regulations and laws

~~SECRET~~

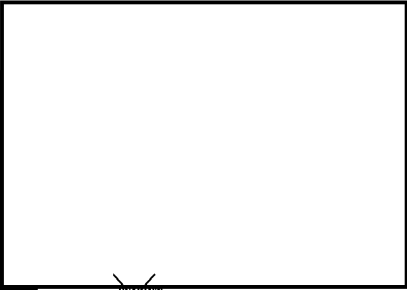
16

b1
b7E

(S)

~~SECRET~~

Suggestions



~~SECRET~~

(S)

~~SECRET~~

Proliferation matters



- Joint cases with Commerce



~~SECRET~~

18

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//OC, NF~~

7/13/2011

~~SECRET~~

Espionage matters

- Reporting requirements and approval authorities are different
 - ◆ Quarterly reports
 - ◆ Interview approvals
 - ◆ 302s
 - ◆ Closing needs HQ approval
- Referrals from other agencies; what to open
- Jurisdiction, especially with military personnel (MOUs)
- Contact with local AUSA (need HQ approval)

~~SECRET~~

19

~~SECRET~~

Economic Espionage

- Need to show [redacted] case needs to protect it
- 284 – Economic CI
 - ◆ Foreign power nexus needed
 - * If none, Intellectual Property case?
 - ◆ Check reporting requirements
- 285 – Acts of Economic Espionage
 - ◆ Criminal matter
 - ◆ Work with AUSA

~~SECRET~~

20

b7E

~~SECRET~~

Considerations...

- ◆ Lead time to HQ [redacted]
- ◆ Manpower intensive, especially in small office
- ◆ Accuracy and minimization reviews [redacted]
- ◆ Files, sub-files, dissemi
- ◆ Volume of product (especially computers)
- ◆ Results; is it worth it?
- ◆ Databases [redacted] not user friendly.
- ◆ Know the rules and systems yourself
- Not meaning to discourage anyone; just FYI...

~~SECRET~~

21

(S)

~~SECRET~~

~~SECRET~~

b1
b7E

~~SECRET~~

Critical National Assets

- Systems, processes, technologies, information critical to US national and economic security
 - ◆ Not the same as critical infrastructure
 - ◆ Do you have any?
 - ◆ [redacted] should advise
 - ◆ Need [redacted]
 - ◆ Joint-use service element
 - ◆ Advise HQ of cases involving CNAs

~~SECRET~~

23

~~SECRET~~

Domain

- Domain coordinator
 - ◆ Key person
 - ◆ Lead for liaison with entities
 - ◆ Working Groups [redacted]
 - ◆ Good relationships = trip wires [redacted]

~~SECRET~~

24

b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~//OC, NF

7/13/2011

(S)

~~SECRET~~

Joint matters

- ◆ It's all about people, not agencies
- ◆ They gain more than we do, but what can they offer
- ◆ Share but keep HQ advised
- Task Forces
 - ◆ MOUs
 - ◆ Sharing

~~SECRET~~ 25

~~SECRET~~

Important: Know who your friends are and use them

Other counterintelligence SSAs in the field
HQ
Desk supervisors (yes, they are on your side)
★ Guidance on DIOG/PIG
Ideas
Hired agents on contract

Legal advice
Not on an island; ask others for opinions/help
all the time

~~SECRET~~ 26

b1
b7E

~~SECRET~~

Comments, thoughts or questions?

~~SECRET~~ 27

~~SECRET~~

~~SECRET~~ 28

~~SECRET~~

~~SECRET~~ 29

~~SECRET~~

~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012

~~SECRET~~

Federal Bureau of Investigation

Integrating Intelligence into
Counterintelligence Operations



~~SECRET~~

1

~~SECRET~~

Counterintelligence Operations and Intelligence

- Very similar in nature
 - CI program has had the least problems with DI initiatives
 - Been doing it for many years
 - Complement each other
- Keys are:
 - SSA/EM involvement and support
 - Setting expectations
 - Not being afraid of the FIG
- Two-way street, both sides need to help each other.

~~SECRET~~

2

~~SECRET~~

~~SECRET~~

3

~~SECRET~~

~~SECRET~~

4

b7E

~~SECRET~~

FIG agents and a CI squad

- Can be a tremendous value
 - Force multiplier
 - Leads related to FI
 - Potential leads for your squad
- Include in squad/program meetings
 - Deconflict
 - Loss of control concerns?

~~SECRET~~

5

~~SECRET~~

FIG analysts and a CI squad

- A good Intelligence analyst is invaluable
 - Intelligence requirements and gaps
 - Preparing
 - Updating
 - Training
 - Production LHM
 - Treat your reports people very well and debriefings? Asset meetings?
 - Need to protect and respect
 - Not an IOA, SOS or regular support
 - Let them what you want, read what they give

~~SECRET~~

6

b7E

~~SECRET~~

~~SECRET~~



- ◆ Approved by HQ
 - ★ SSA role; if you like it, tell HQ
- ◆ Read the drafts; they represent your program
 - ★ Make changes or cancel if not of quality
- ◆ Operational considerations
 - ★ Ops take priority over disseminations, but always keep disseminations in mind
 - ★ Have an IA review cases on occasion; might be some forgotten intel in them
- ◆ Production is important; numbers count!

~~SECRET~~

7

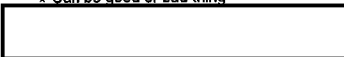
~~SECRET~~



- ◆ Finished intelligence product
 - ★ Relevant local intelligence



- ◆ Approved by SAC
 - ★ Can be good or bad thing



~~SECRET~~

8

b7E

~~SECRET~~



- ◆ CI SSA needs to be involved in drafting

Valuable for:

- SAC brief
- SAPR



~~SECRET~~

9

~~SECRET~~



~~SECRET~~

10

b7E

~~SECRET~~

Accountability for agents

- Metrics for all to see



- Files reviews
- Performance plans
- Make it clear ahead of time what you expect
 - ◆ Now it's up to them

~~SECRET~~

11

~~SECRET~~

Summary

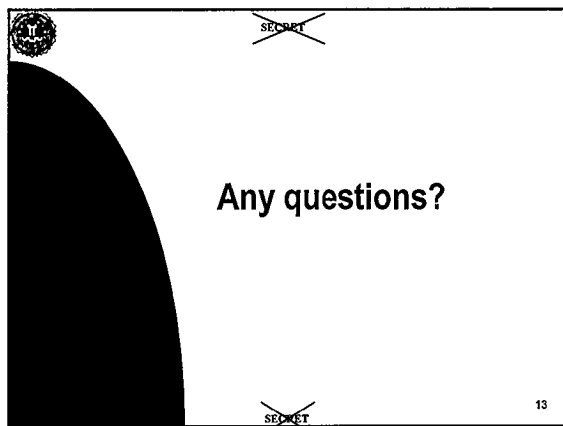
Counterintelligence has the best potential for coordinated efforts with intelligence

- ◆ Other programs not as well-suited
- ◆ Open to working with the FIG
- ◆ Analysts are invaluable
- ◆ Need to give back to the FIG

~~SECRET~~

12

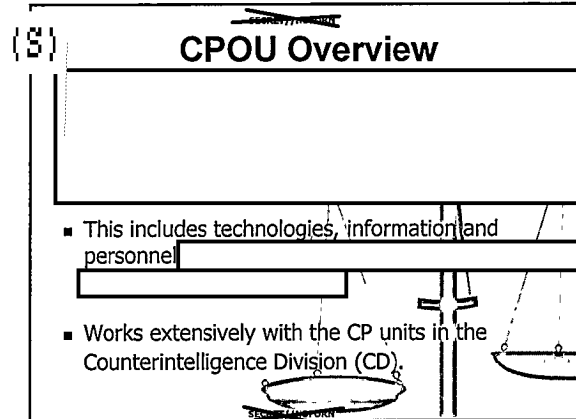
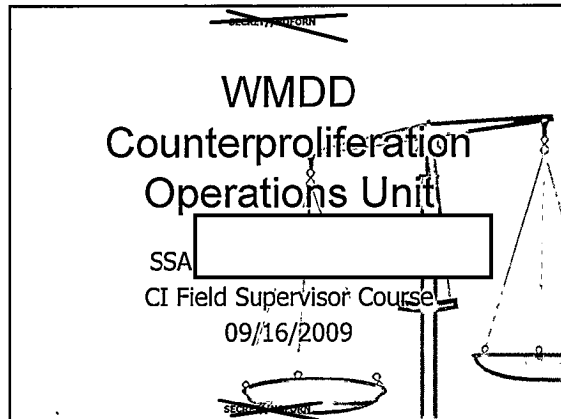
b7E



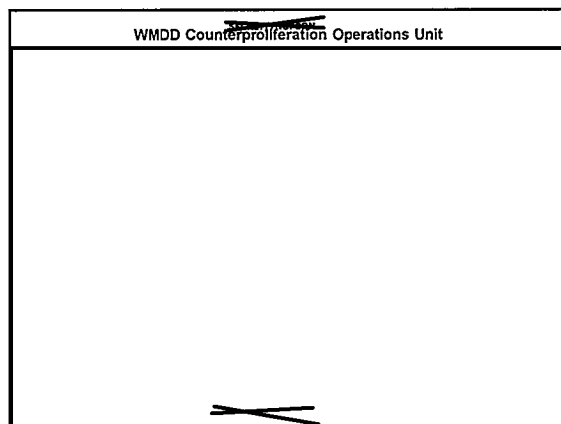
DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

~~SECRET~~

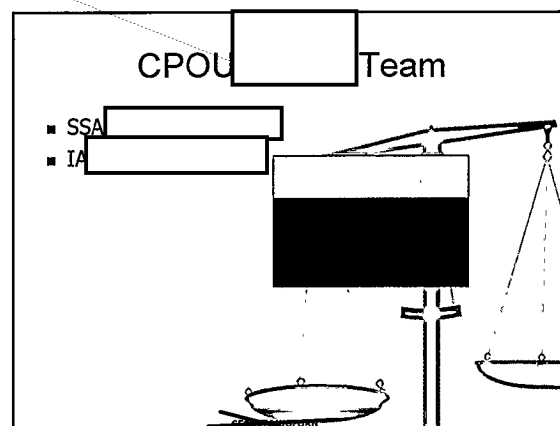
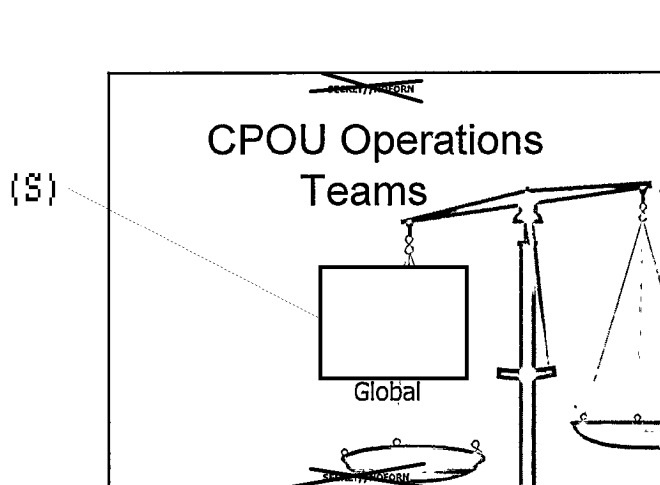
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b1
b6
b7C
b7E



b6
b7C
b7E



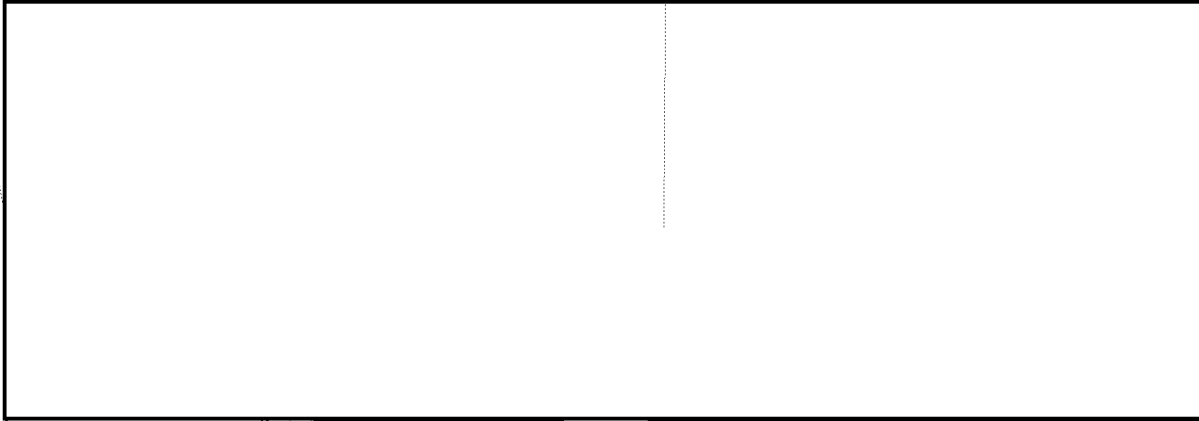
b1
b6
b7C
b7D
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

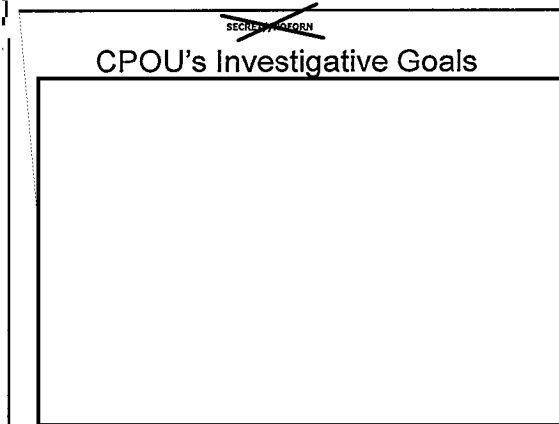


b1
b7D
b7E

(S)



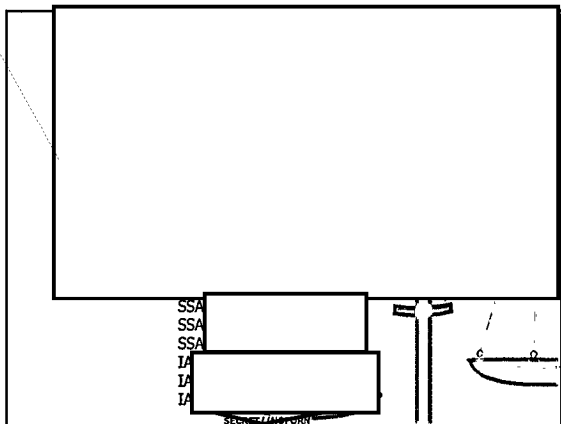
(S)



b1
b7D
b7E

(S)

(S)



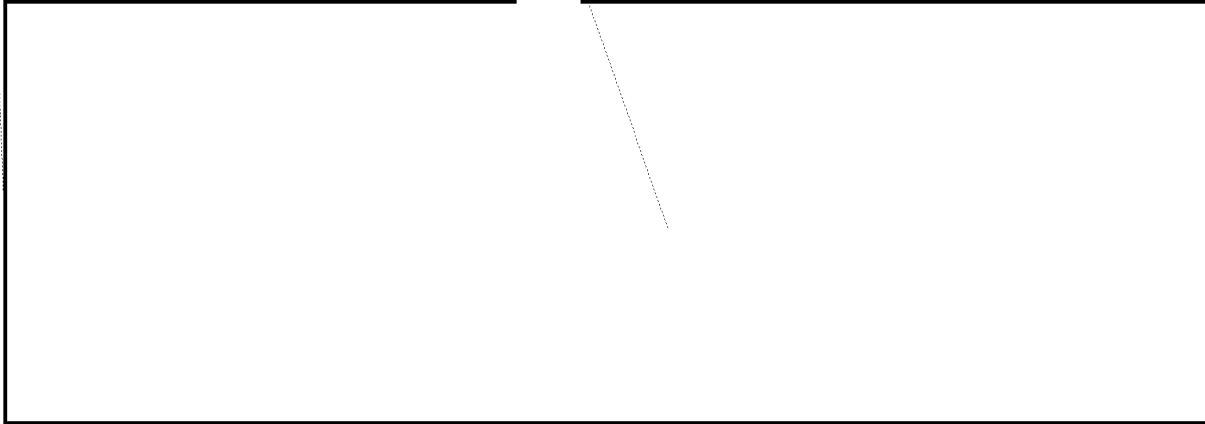
b1
b6
b7C
b7D
b7E

~~SECRET~~

~~SECRET~~

(S)

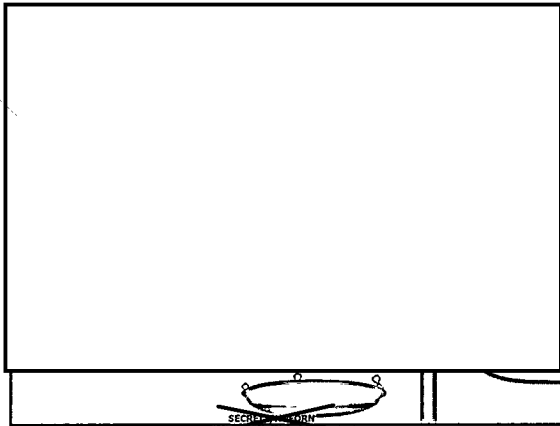
(S)



b1
b7D
b7E

(S)

(S)



SECRET//NOFORN

CPOU Programs and Personnel

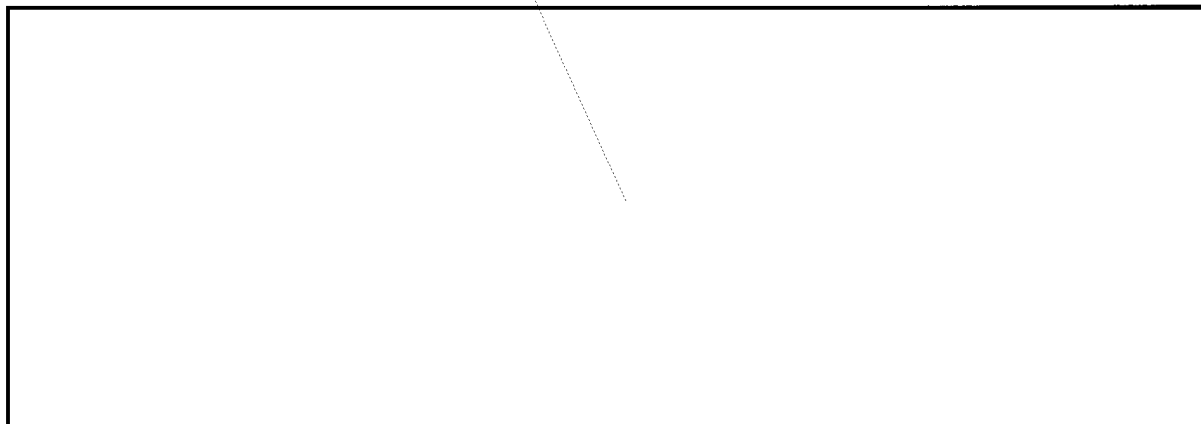
- Proliferation Security Initiative (PSI)
- Chemical Weapons Convention (CWC)
- CP Coordinators
- CP Field Analysts
- Detailees

A small diagram of a balance scale is located at the bottom right of the slide. It is partially redacted.

b1
b7D
b7E

(S)

(S)



b1
b7D
b7E

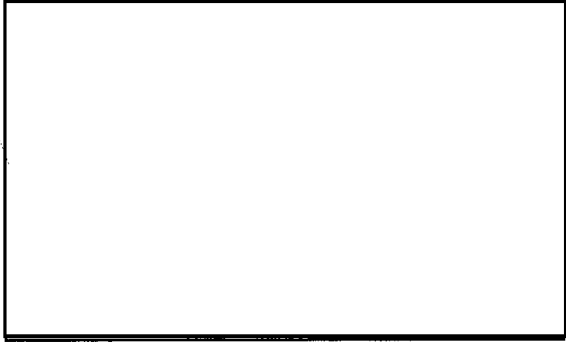
~~SECRET~~

~~SECRET~~

(S)

~~SECRET//NOFORN~~

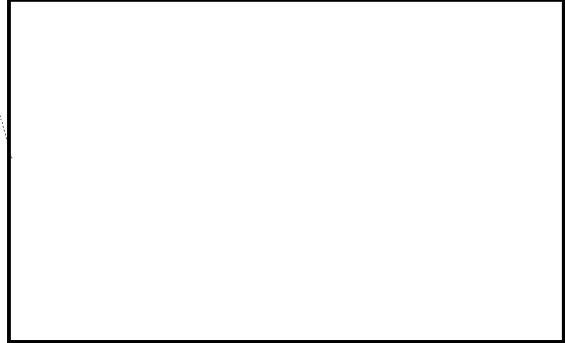
Result



(S)

~~SECRET//NOFORN~~

What it means



b1
b7E

(S)

~~SECRET//NOFORN~~

Expectation Management



(S)

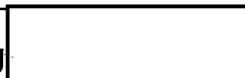
~~SECRET//NOFORN~~

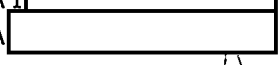
Upcoming Collections

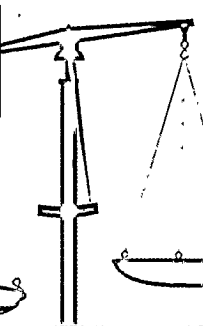


b1
b7D
b7E

(S)

CPOU  **Team**

- SSA 
- IA I 
- IA 



~~SECRET//NOFORN~~

Proliferation Security Initiative (PSI)

- Originally launched by President Bush in 2003, the Proliferation Security Initiative (PSI) is an international agreement designed to prevent the proliferation of WMD, precursors and components.
- Currently, 95 countries participate in PSI and collectively utilize existing state and international laws to prevent WMD proliferation.
- National Security Council Oversight.



b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

FBI 2009 Engagements with PSI

- May 2009 Operational Experts Group (OEG) meeting, Miami, FL, and included a regional outreach with 10+ South American countries.
- July 2009 PSI workshop, Budapest, Hungary, engaged 8 Middle Eastern countries.
- September 2009 PSI workshop, Sydney, Australia, engaging 10+ Asian countries.
- February 2010 - PSI Exercise "Leading Edge" Abu Dhabi, UAE, to include Port and Tabletop Interdiction Exercises.

CPOU PSI Team

- SSA [redacted]
- SSA [redacted]
- SSA [redacted]

b6
b7C
b7E

Chemical Weapons Convention (CWC)

What is the CWC?

- CWC is an international arms control agreement that prohibits the development, production, acquisition, stockpiling, transfer and use of chemical weapons (CW)
- Ratified by 188 countries
- Each country is required to allow inspections of declared CW and precursor facilities
 - In the US, inspection occur at both military destruction and storage facilities as well as commercial facilities

Example of Threat by CWC Inspectors

- The most common threat during a commercial inspection is attempts by inspectors to access confidential business information outside the scope of the inspection for various reasons
 - Economic espionage
 - Directed by a foreign intelligence service
 - Genuine curiosity

(S)

(S)

FBI's Role in CWC

- FBI is mandated by Congress to participate in CWC inspections of US commercial facilities in order to protect confidential business information
 - FBI is not required to accompany DoD at the military facilities
 - Department of Commerce (DOC) has the lead for commercial inspections
- CPOU coordinates the local FBI field office response and participation in CWC inspections
 - Less than 1 week notice is given for each inspection
 - Local FBI provides an SA to accompany each DOC inspection team and provide a pre-inspection and counterintelligence awareness briefing
- In 2008, there were 19 inspections at commercial facilities

b1
b7E

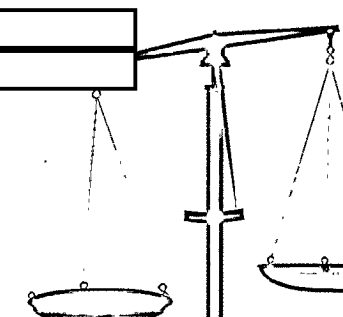
~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

CPOU CWC Team

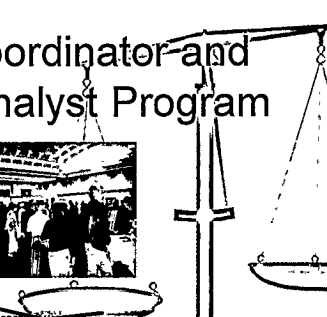
- SSA [redacted]
- IA [redacted]



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

CP Coordinator and Field Analyst Program



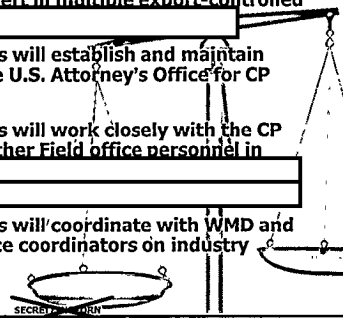
~~SECRET//NOFORN~~

b6
b7C

~~SECRET//NOFORN~~

CP Coordinators Program

- Field office expert in multiple export-controlled [redacted]
- CP coordinators will establish and maintain liaison with the U.S. Attorney's Office for CP matters
- CP coordinators will work closely with the CP Analysts and other Field office personnel in identifying [redacted]
- CP coordinators will coordinate with WMD and other field office coordinators on industry outreach



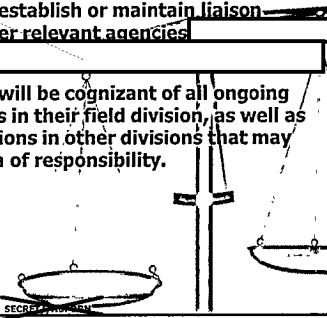
~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

CPOU – CP Coordinators

- CP coordinators establish or maintain liaison contact with other relevant agencies [redacted]
- CP coordinators will be cognizant of all ongoing CP investigations in their field division, as well as major investigations in other divisions that may impact their area of responsibility.



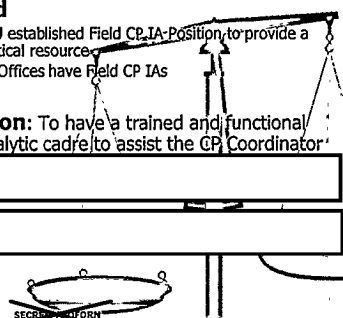
~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

Field CP Analyst Program

- **Background**
 - In 2007, CPOU established Field CP IA Position to provide a Field CP analytical resource
 - Over 40 Field Offices have Field CP IAs
- **CP IA Mission:** To have a trained and functional Field Office analytic cadre to assist the CP Coordinator

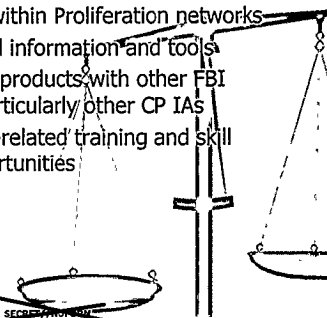


~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Field CP IA Roles and Responsibilities

- Identify trends within Proliferation networks
- Share CP-related information and tools
- Share analytical products with other FBI components, particularly other CP IAs
- Identify new CP-related training and skill acquisition opportunities



~~SECRET//NOFORN~~

b7A
b7E

~~SECRET~~

~~SECRET~~

Field CP IA Network

- CPOU has hosted 2 CP Analytical Conferences to support this program (Quantico-July 2007 and Crystal City- August 2008)
- Field CP Analysts also recently participated in the MEGA Conference (Sandia National Laboratory-May 2009)
- Working with other WMDD components to host CP Conference for FY 2010.

CP Coordinator and Analyst Programs

- SSA [redacted]
- PM [redacted]

b6
b7C

CPOU Detailees

Strategic Interdiction Group (SIG)

- Identify, penetrate, and disrupt WMD-related proliferation networks
 - Network Analysis
 - Targeting and Operations

b1
b7E

Interagency Planning and Coordination

- Support the coordination and synchronization of interdiction activities across U.S. Government
 - M-W-F Interagency meetings to facilitate interdiction coordination
 - Weekly Interdiction Sub-PCC/IPC
 - Daily integration due to co-location
- Liaison with policy, intelligence, military, and law enforcement agencies (and relevant interagency committees)
- Strategic interdiction planning
 - Strategic Interdiction Studies/Critical Technology
 - Interagency Supplier Denigration
- Detailees or Liaison officers

FBI Involvement

- Expand the range of options [redacted]
- Improve information sharing [redacted]
- Coordinate more closely with domestic counterparts for the interdiction and investigation of WMD Counterproliferation
- Integrate LEGATS to assist in international interdiction efforts
- Obtain additional analytical support to key cases [redacted]

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

b1
b6
b7C
b7D
b7E

CPOU SIG Detailees

- SSA [redacted]
- SSA [redacted]

US Department of State Directorate of Defense Trade Control (DDTC)

- The Department of State, Directorate of Defense Trade Controls (DDTC), is responsible for administering the Arms Export Control Act (AECA) and its regulations, the International Traffic in Arms Regulations (ITAR)
- The ITAR regulates the export of defense articles, defense services and brokering activities

b6
b7C
b7E

(S)

The FBI's Role

- On 11/05/2004, the Attorney General signed an order clarifying FBI criminal jurisdiction in export matters with a counterintelligence nexus.

As written, the order designates "the FBI to take charge of investigative work in matters relating to espionage, sabotage, subversive activities, and related matters, including investigating any potential violations of the Arms Export Control Act, the Export Administration Act, the Trading with the Enemy Act, or the International Emergency Economic Powers Act, relating to any foreign counterintelligence matter".

Title 28, Chapter 1, Part 0, Subpart 0, Section 0.00, para (a) and para (b) - effective 11/15/2004

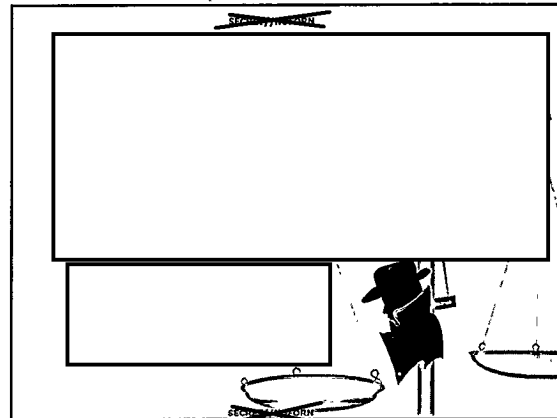
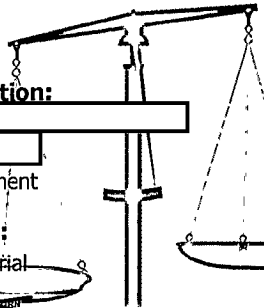
b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~
Certification

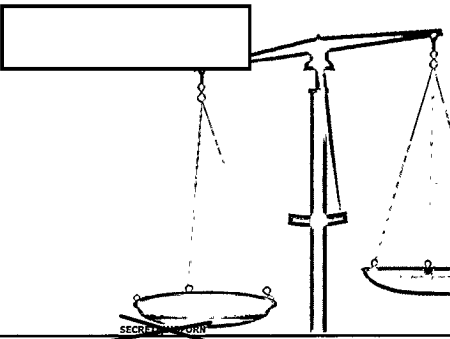
- **Level I:**
 - Cursory review
- **Pre-trial Certification:**
 - In-depth analysis: [redacted]
 - Required for indictment
- **Trial Certification:**
 - Required prior to trial



b7E

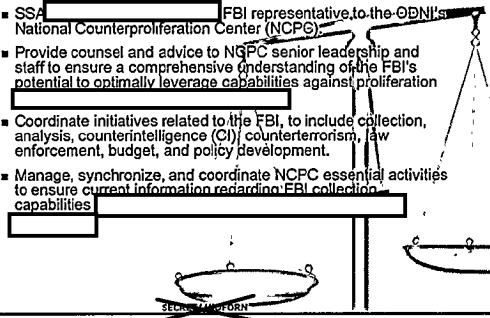
~~SECRET//NOFORN~~
CPOU DDTC Detailee

- SSA [redacted]



~~SECRET//NOFORN~~
WMDD/CPOU – Detailee to National Counterproliferation Center (NCPC)-Intelligence and Action Integration (IAI)

- SSA [redacted] FBI representative to the ODNI's National Counterproliferation Center (NCPC)
- Provide counsel and advice to NCPC senior leadership and staff to ensure a comprehensive understanding of the FBI's potential to optimally leverage capabilities against proliferation
- Coordinate initiatives related to the FBI, to include collection, analysis, counterintelligence (CI), counterterrorism, law enforcement, budget, and policy development.
- Manage, synchronize, and coordinate NCPC essential activities to ensure current information regarding FBI collection capabilities

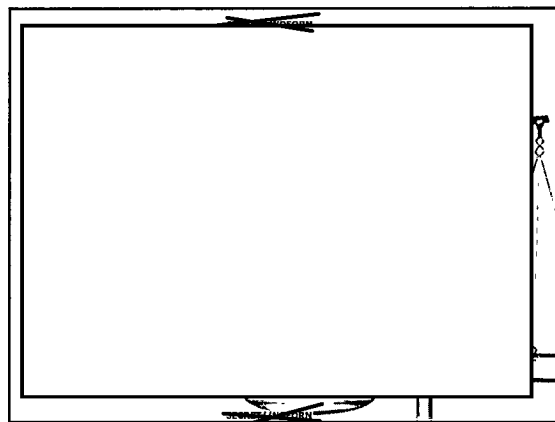


b6
b7C
b7E

~~SECRET//NOFORN~~
WMDD/CPOU – Detailee to National Counterproliferation Center (NCPC)-Intelligence and Action Integration (IAI)



(S)



b1
b7E

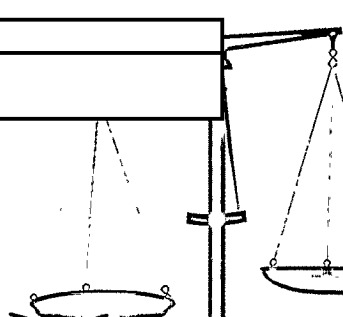
~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

CPOU [redacted] Detailees

- SSA [redacted]
- IA [redacted]
- IA [redacted]

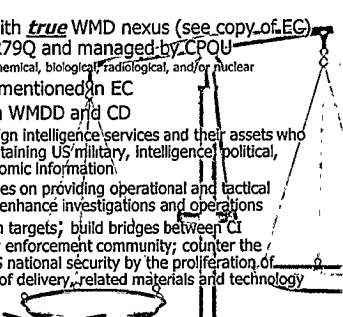


~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

What to Remember

- All new CP cases with true WMD nexus (see copy of EC) will be opened as 279Q and managed by CPOU
 - 51% WMD nexus, i.e. chemical, biological, radiological, and/or nuclear
- Details specifically mentioned in EC
- Difference between WMDD and CD
 - CD focuses on foreign intelligence services and their assets who are dedicated to obtaining US military, intelligence, political, scientific, and economic information.
 - WMDD/CPOU focuses on providing operational and tactical analytic support to enhance investigations and operations against proliferation targets; build bridges between CI community and law enforcement community; counter the threats posed to US national security by the proliferation of WMD, their means of delivery, related materials and technology



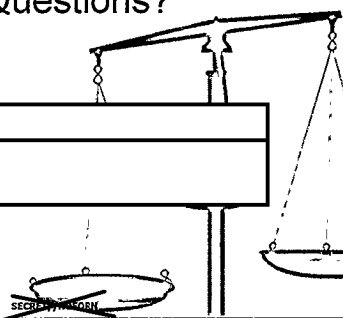
~~SECRET//NOFORN~~

b6
b7C
b7E

~~SECRET//NOFORN~~

Questions?

SSA [redacted]



~~SECRET//NOFORN~~

b6
b7C
b7E

~~SECRET~~

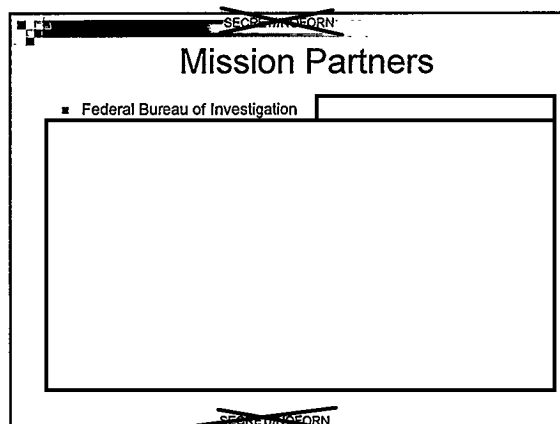
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



NCIJTF Mission

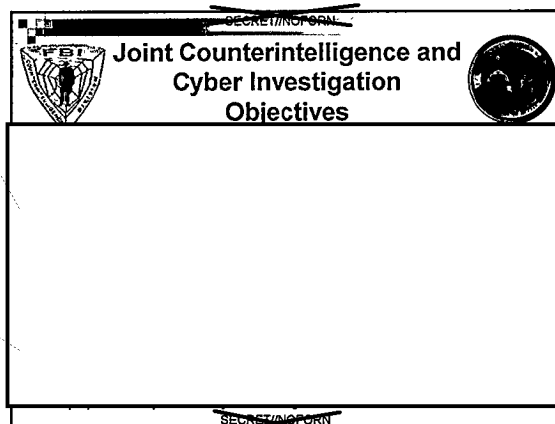
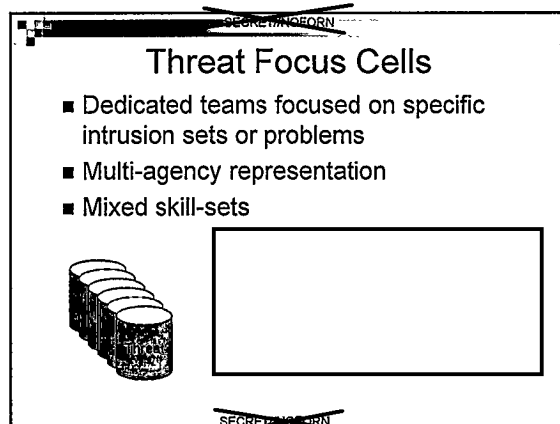
The National Cyber Investigative Joint Task Force (NCIJTF) identifies, mitigates, and disrupts cyber threats by coordinating and integrating the counterintelligence, counterterrorism, intelligence, and law enforcement activities of member organizations.



NCIJTF End State

- The NCIJTF is an alliance of peers with complementary missions to protect national cyber interests.
- The NCIJTF provides participating agencies with value-added information in a collaborative environment without directing the operational or investigative responsibilities of participating agencies.
- Operations and investigations coordinated through the NCIJTF are built upon the complementary authorities of its membership.

b7E



b1
b6
b7C
b7E

~~SECRET~~
ACLURM043239

~~SECRET~~

(S)

(S)

b1
b7D
b7E

What is the Threat?

(U) The Internet is a system built on trust that users, data, and applications at the network's endpoints know and trust one another. The Internet delivers packets whether they are legitimate or the electronic equivalent of letter bombs.

(U) Users trust that:

- > email is secure, confidential, and reliable
- > public websites are trusted
- > applications are coded from a trusted and authorized vendor or developer
- > protocols and standards are trusted and fair for the benefit of all

(S)

2008 Global Internet Traffic Map

b1
b7E

Internet Core

The "Internet Core" is a collection of private carrier networks that provide higher level of service for the global coverage of the Internet.

Rank	ISP	Rank	ISP
1	Verizon	1	Verizon
2	AT&T	2	AT&T
3	Sprint	3	Sprint
4	Comcast	4	Comcast
5	Qwest	5	Qwest
6	Time Warner	6	Time Warner
7	Earthlink	7	Earthlink
8	Level 3	8	Level 3
9	Charter	9	Charter
10	Suddenlink	10	Suddenlink

Significance of Trans-Oceanic Fiber Cables

(U//FOUO) Undersea fiber-optic cables form the backbone of the international telecommunication network and carry more than 95 percent of international voice and data traffic and supply secure, high-speed, large-capacity transmissions for both military and commercial communications.

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

Regulation of the Internet

(U) The Internet and its system of protocols began in the 1970's by the U.S. Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF).

(U) No one is truly in charge of the Internet; new applications, lines, and routers are added continually by thousands of companies, none of which require permission from anybody, and none of which are obliged to report their activities.



(U) Governments are wrestling with jurisdiction issues. These will settle out over the next decade and increase/decrease freedom, drive industries to less regulated locations, etc. (e.g., gambling, China censorship, items of type X cannot be sold in country Y on eBay, etc.).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Internet Society and the IETF



~~SECRET//NOFORN~~

b7E

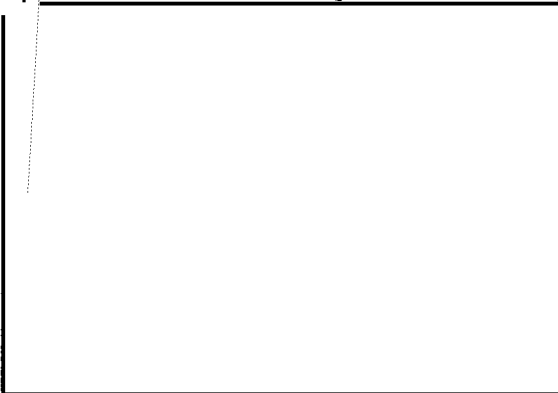
~~SECRET//NOFORN~~

IETF



(S)

(S) ~~SECRET//NOFORN~~



b1
b7E

~~SECRET//NOFORN~~

NCIJTF Vendor and Telecom Working Group



(S)

~~SECRET//NOFORN~~

Questions?

SSA 



Unclass Email: 

 Email: 

 Email: 

~~SECRET//NOFORN~~

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~



Economic Espionage

September 14, 2009

ECONOMIC ESPIONAGE ACT OF 1996

- 18 U.S.C. 1831
 - Economic espionage
 - (Foreign power)
- 18 U.S.C. 1832
 - Theft of trade secrets
 - (No foreign power)



b7E

ELEMENTS COMMON TO 1831 & 1832



THE GOVERNMENT MUST PROVE:

- The defendant misappropriated information
- The defendant knew that the information was a trade secret
- The information was a trade secret

MISAPPROPRIATION

- *VERY BROAD, TO INCLUDE:*
 - Fraud or deception
 - Altering or destroying
 - Receiving, buying, possessing . . . with knowledge

CLEVELAND CLINIC & RIKEN



Charges:

- EEA: Taking, Altering & Destroying
- ITSP
- False Statements
- Conspiracy



b6
b7C

~~SECRET~~

WHAT IS A TRADE SECRET?



A TRADE SECRET IS INFORMATION WHICH THE OWNER . . .

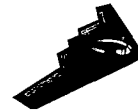
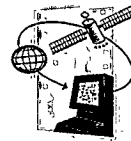
- Has taken reasonable measures to protect
 - And
- It derives independent economic value from not being generally known, or readily ascertainable, by the public

TRADE SECRETS MAY INCLUDE:

- Financial, business, scientific, engineering information
- Patterns, plans, formulas, methods, prototypes
- Whether tangible or intangible

REMEMBER

The information / technology does not have to be high-tech to be a trade secret!



ADDITIONAL 1831 ELEMENT

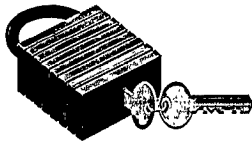
- Intend to or knowingly benefiting
 - foreign government or
 - foreign instrumentality



EXTRATERRITORIALITY

- Defendant is a U.S. citizen or PRA
- Entity organized under U.S. law
- Act in furtherance was committed in the U.S.



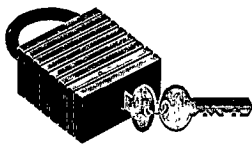


Companies often ask:
“*Will Our Trade Secrets Stay
Secret At Trial?*”



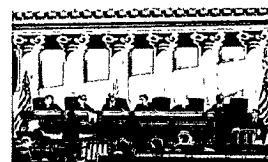
BRISTOL-MEYERS SQUIBB

“The Taxol Case”



18 U.S.C. 1835

“... the court *shall* enter such orders
and take such other action ... to
preserve the confidentiality of trade
secrets ...” (*emphasis added*)



U.S. v. HSU, 155 F.3d 189
(3rd Cir. 1998)

Third circuit overruled the PA district
court and ordered that trade secrets
shall be confidential



PENALTY



- 1831 - person: 15 years & \$500,000 fine
corp: \$10,000,000 fine
- 1832 - person: 10 years & \$250,000 fine
corp: \$5,000,000 fine

HOW DO WE GET THESE
CASES?

TAKE-AWAYS

- Must have a trade secret to make an EE case
- Must have a foreign power nexus to make an 1831 case
- Subject does not have to be taking direction from the foreign power
- is your POC for all matters EE and IEEPA

FBIHQ

b6
b7C
b7E



THANK YOU

How Scientists View Law Enforcement

New Survey of Researchers Tells Us How to Help the Communities Communicate

By Nathaniel Hafer,* Cheryl J. Vos,* Karen McAllister, Gretchen Lorenzi,
Christopher Moore, Kavita M. Berger, and Michael Stebbins

February 2009

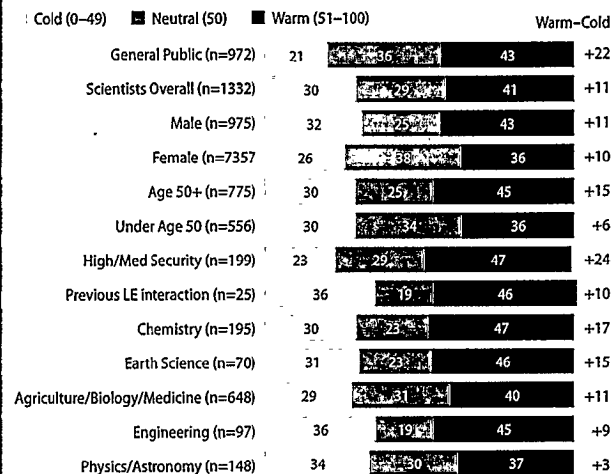
ANECDOTAL EVIDENCE, including several high-profile cases of scientists under criminal investigation, has led to the impression that many in the scientific community hold a negative view of law enforcement.^{1, 2, 3} While justified in some cases, this divide is a serious liability to law enforcement, since cooperation and consultation with scientists aids in threat assessment, investigation, intelligence gathering, and the recruitment of personnel with specialized skills. But before the two communities can solve this problem with training for law enforcement personnel and through outreach to the scientific community, it is necessary to get a sense of the types and range of views of law enforcement within the scientific community.

Here we present the results of a survey of the scientific community conducted in conjunction with the FBI to evaluate the working relationship between FBI field agents and scientists. The survey was sent to 10,969 members of the American Association for the Advancement of Science between January 23 and February 18 of this year. 1,332 surveys were completed, and the resulting data produced an average margin of error associated with the total data set of ± 2.7 percent. A complete version of the survey questions is available in the supplemental material (Table 1).

The attitudes of scientists toward law enforcement personnel are not vastly different from those of the general public (Figure A).⁴ However, a larger percentage of scientists indicated cooler feelings towards the FBI than the general public, suggesting that these reservations are particular to the scientific community and require specific solutions with the scientific community in mind.

FIGURE A

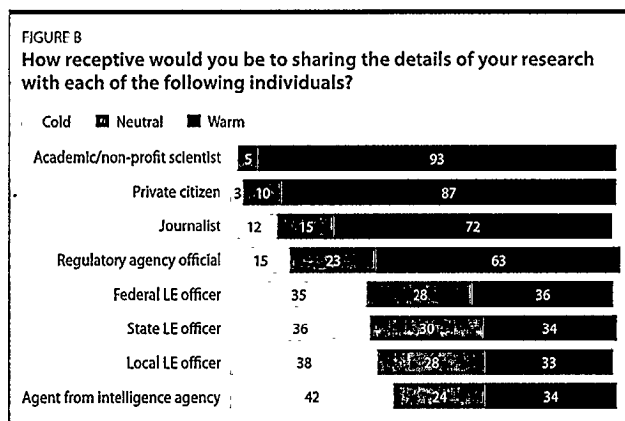
Please indicate your feelings towards the FBI.



Figures A, B, C, and E: Responses to selected questions from the survey; the complete list of survey questions is in Figure D. For Figures A and B, a complete explanation of the thermometer rating system is in the Methods. For Figure C, responses of very receptive or somewhat receptive responses are labeled warm, responses of neither receptive nor unreceptive are labeled neutral, and very unreceptive or somewhat unreceptive responses are labeled cool. For Figure E, scientists were asked this question in an open-ended format and were allowed to list multiple suggestions. As a result the percentages do not sum to 100.

The results show that scientists hold more favorable feelings towards state and local law enforcement than federal law enforcement. However, when confronted with specific issues or concerns, the responses reveal no significant distinction between interact-

ing with the FBI or with law enforcement in general. Generally speaking, working in a specific scientific discipline has less effect on an individual's view of law enforcement than demographic factors. Instead, trends suggested that male scientists and those over 50 years of age have a more positive attitude towards the FBI (Figure A). It should be noted that those scientists holding high or medium security clearances—and therefore arguably more likely to have firsthand contact with federal agents—had the highest level of warm views (47 percent) and the lowest level of cool views (23 percent) toward the FBI of any cohort covered in the survey. The survey also revealed that scientists are receptive to the idea of discussing their research with other scientists (93 percent), interested members of the public (87 percent), and journalists (72 percent), but are markedly unreceptive to sharing their work with law enforcement (federal 36 percent, state 34 percent, local 33 percent) (Figure B).



Perhaps the most striking of the results is the indication that scientists are suspicious of the FBI and feel that they do not work well with the scientific community. Some scientists who had professional interactions with law enforcement reported that they had been questioned about the purpose of their international travel, asked to "spy" on their foreign colleagues, and in one case had a computer confiscated and searched. Specific concerns include the belief that law enforcement does not understand their work (76 percent), the belief that law enforcement is more interested in restricting research for security purposes than they are in the scientific value of the work (71 percent), that law enforcement has an overzealous approach to security issues and an interest in censorship (63 percent), and the fear that law enforcement will restrict the publication of some research (55 percent).

Scientists expressed a clear preference to leave the monitoring of science to familiar authorities rather than law enforcement. Figure C illustrates that most scientists find it acceptable for a familiar authority such as an institutional biosafety committee (64 percent), institutional review board (63 percent), the head of the department

(70 percent), or a government funding agency (60 percent) to play a role in monitoring research. In contrast, there is resistance to FBI (14 percent favorable), state law enforcement (13 percent favorable), local law enforcement (11 percent favorable), private security (11 percent favorable), or campus police (11 percent favorable) playing any role. Despite this reluctance to be monitored by law enforcement, scientists were not completely unwilling to interact with authorities in certain circumstances. The survey asked scientists to consider different circumstances where they might be asked to interact with the FBI and evaluate whether they felt the reasons for contact were good or bad (Figure D).

Almost all respondents (93 percent) felt that requesting technical expertise in a particular area of science was an excellent or good reason to be contacted, and 80 percent agreed that aiding in an ongoing criminal investigation was an excellent or good reason to work with law enforcement. However, the survey revealed that scientists are generally concerned that they would be asked to monitor the activities of a colleague, which 67 percent felt is not a legitimate reason to be contacted by the FBI. Understandably, scientists looked unfavorably on any role that law enforcement might have which interferes with research (57 percent); funding (52 percent); that invades privacy, such as reading personal emails (62 percent); or provides any role for law enforcement to interpret legitimate research as a potential public safety risk (61 percent).

Although some level of suspicion or distrust toward the FBI exists within the scientific community, it is interesting to note that only 15 percent of the surveyed scientists indicated any personal past contact with law enforcement agents in a professional capacity. The general view of these scientists towards the FBI was not significantly different from the views of scientists overall (Figure A), however they are more comfortable reporting suspicious activity to the authorities. Seventy-one percent of those

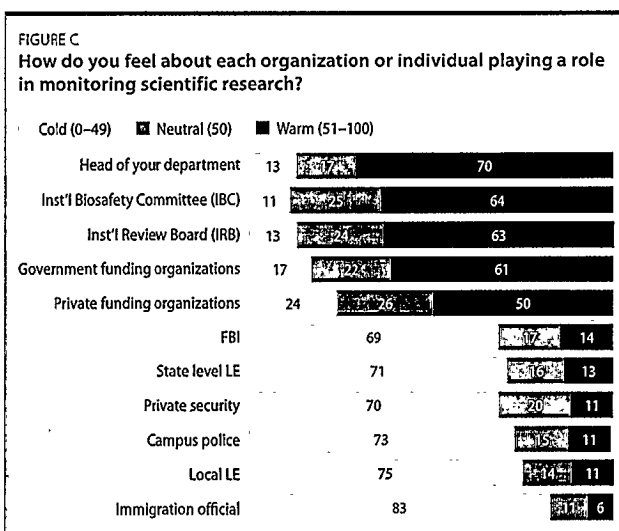
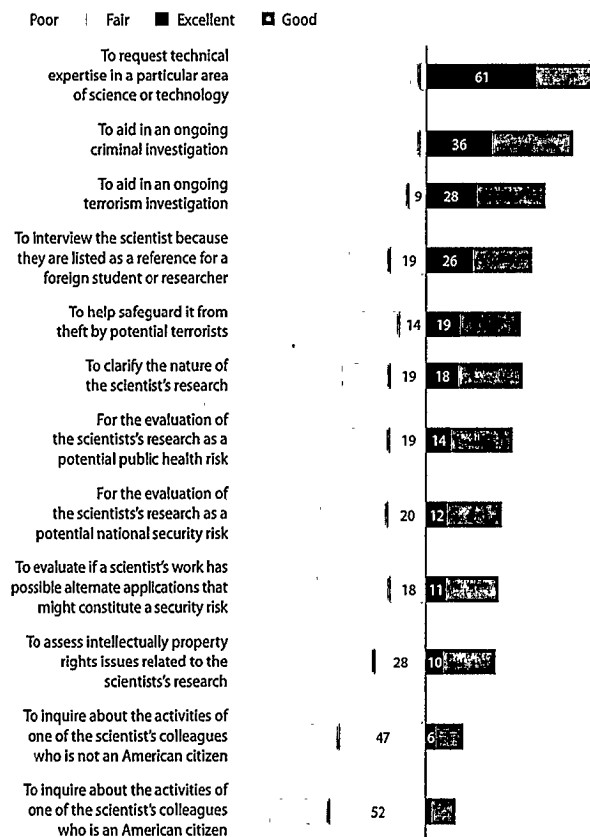


FIGURE D

List of responses from scientists answering the question, "There are many reasons that an FBI agent might want to talk with a scientist. For each of the following, please indicate whether you believe it is an excellent, good, fair, or poor reason for an FBI agent to approach a scientist."



who had previous interaction with law enforcement indicated that being contacted as a reference for a foreign student or researcher was a good or excellent reason, as opposed to 58 percent of those who had not. It is likely that this is a result of previous experience, since 30 percent of survey respondents reported that their past interaction with law enforcement was in regard to a visa or security clearance for themselves or a colleague. Nonetheless, the low percentage of scientists with previous law enforcement contact suggests that many of the attitudes of distrust are based upon stereotypes rather than actual experiences and that these perceptions have led to an elevated level of suspiciousness that law enforcement will have to overcome in the future. Together the results show that despite expressed suspicions of the FBI and opposition to law enforcement monitoring research, scientists are willing to aid law enforcement in certain situations. When asked in an open-ended context about what the FBI could do to improve relations with the scientific community, no single solution emerged (Figure E). A common suggestion from the respon-

dents was to set up an appointment and approach the scientist in a professional manner. Respondents also stated that it would be beneficial for authorities to first contact the individual's department head or supervisor and initiate contact through an institution's official channels.

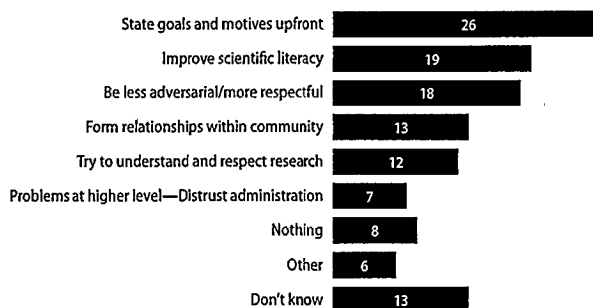
By taking steps to address suspicions early in any interaction and by treating scientists respectfully and professionally, law enforcement representatives are more likely to build a foundation of respect with their interaction and displace existing hostility. Perhaps the single most important step would be to adopt simple procedures for an introductory phone call, email, or letter that clarifies the specific purpose for the meeting and details what the agent hopes to gain from the interaction. To ease the concerns expressed by scientists regarding their collaborators or their privacy, it is imperative that an agent establish clear boundaries about what they plan to do and plan not to do in any interaction. Being clear about the purpose of the meeting should alleviate suspicions and increase the likelihood of full cooperation.

Many scientists indicate that an understanding of science by an agent would ease their suspicions and therefore it may be helpful to increase the scientific literacy of law enforcement agents. Among researchers who felt that an official from law enforcement understood their work, 81 percent were receptive to helping in a criminal investigation, while only 63 percent of researchers who felt that a law enforcement official did not understand their work were receptive to helping. From this we conclude that scientists are most comfortable talking about their work to others that demonstrate familiarity with scientific concepts, possibly because they are less concerned that their work will be misunderstood.

Our survey shows that scientists share many of the common stereotypes held of law enforcement by the general public. More interestingly, it elucidates some issues that are specific to the science community, such as a general expressed reluctance to discuss research with law enforcement, despite an expressed willingness to

FIGURE E

What can LE do to improve relations with the scientific community? Percentage of respondents



share expertise to aid in criminal investigations. Increasing scientific literacy among law enforcement personnel who work with scientists may be one important avenue to ensure a strong relationship and clear communication between the law enforcement and science communities. The consequences of allowing discord between law enforcement and scientists to linger affect public safety as criminal, terrorist, and national security challenges become increasingly technical, and close collaboration with the scientific community becomes even more essential. We hope to apply the lessons learned in this survey towards improving the training and awareness of the law enforcement community in their interaction with scientists.

METHODS

THE SURVEY—The Federation of American Scientists, in collaboration with the Federal Bureau of Investigation and Greenberg Quinlan Rosner Research, developed a survey to gather baseline data on the prevailing points of view of scientists towards the law enforcement community. The survey contained a mix of multiple choice and open-ended questions. In collaboration with the American Association for the Advancement of Science the survey was distributed to 10,969 AAAS member scientists over a four-week period between January 23 and February 18, 2008. AAAS members were selected if they had a functional email address and had identified their primary field of study as biology, chemistry, physics, earth science, or engineering. Emails contained a link to a secure website where members could answer the survey questions. At the end of

the time period 1,332 surveys were completed, and the resulting data were analyzed. The data were statistically weighted to be proportionally representative of the scientific disciplines of the AAAS membership. The margin of error associated with the total data set is +/- 2.7 percent.

Thermometer rating system – Two survey questions asked respondents to indicate their feelings towards a particular person, organization, or situation using a thermometer system. In this type of question, respondents give their response as any number between 0 and 100, with 100 being a very warm, favorable feeling, and 0 being a very cold, unfavorable feeling, and 50 meaning not particularly warm or cold.

Nathaniel Hafer, Cheryl J. Vos, and Michael Stebbins are with the Federation of American Scientists; Karen McAllister and Gretchen Lorenzi are with the Federal Bureau of Investigation; Christopher Moore is with Greenberg Quinlan Rosner Research; Kavita M. Berger is with the American Association for the Advancement of Science.

**Nathaniel Hafer and Cheryl J. Vos contributed equally to this work. Michael Stebbins is the corresponding author, mstebbins@fas.org*

REFERENCES

- 1 D. Malakoff, *Science*, 297, 751-752 (2002).
- 2 M. Enserink, D. Malakoff, *Science*, 302, 2054-2063 (2003).
- 3 J. Couzin, *Science*, 305, 159 (2004).
- 4 NBC news/Wall Street Journal Survey, June 12, 2006.

ABOUT THE AUTHORS

Nathaniel Hafer, Cheryl J. Vos, Michael Stebbins: The Federation of American Scientists, 1725 DeSales Street NW, Washington, DC 20036.

Karen McAllister, Gretchen Lorenzi: The Federal Bureau of Investigation, 935 Pennsylvania Avenue NW, Washington, DC 20535.

Christopher Moore: Greenberg Quinlan Rosner Research, 10 G Street NE, Washington, DC 20002.

Kavita M. Berger: The American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.

TABLE 1

Complete list of questions asked in the survey

Question 1. Please indicate your feelings toward the following people and organizations with 100 meaning a VERY WARM, FAVORABLE feeling; 0 meaning a VERY COLD, UNFAVORABLE feeling; and 50 meaning not particularly warm or cold. You can use any number from 0 to 100, where the higher the number the more favorable your feelings are toward that person or organization.

Local law enforcement	Institutional Review Board (IRB)
State level law enforcement	Campus police
Federal Bureau of Investigation (FBI)	Head of your department
Institutional Biosafety Committee (IBC)	Private grantmaking organizations
Department of Homeland Security (DHS)	Government grantmaking organizations

Private security, such as those found at private research centers

Question 2. The following people and organizations might have some role in monitoring scientific research under certain circumstances. Please indicate your feelings about each one having some role in monitoring scientific research under certain circumstances, with 100 meaning a VERY WARM, FAVORABLE feeling; 0 meaning a VERY COLD, UNFAVORABLE feeling; and 50 meaning not particularly warm or cold. You can use any number from 0 to 100, where the higher the number the more favorable your feelings are toward that person or organization having some role in monitoring scientific research under certain circumstances.

Local law enforcement	Institutional Review Board (IRB)
State level law enforcement	Campus police
Federal Bureau of Investigation (FBI)	Head of your department
Institutional Biosafety Committee (IBC)	Private grantmaking organizations
Department of Homeland Security (DHS)	Government grantmaking organizations

Private security, such as those found at private research centers

Question 3. From time to time, individuals other than your immediate colleagues might be interested in the work you do. Please indicate how receptive you would be to sharing details of your work for each of the following:

Federal law enforcement agent	State level politician
State law enforcement officer	Federal level politician
Local law enforcement	Private sector scientist
An official from a regulatory agency	Public sector scientist
An agent from an intelligence agency	Academic/non-profit scientist
Corporate executive in a related industry	A journalist

Private citizen with an interest in science

Question 4. There are many reasons that an outside authority might want to talk to you in your role as a scientist. For each of the following, please indicate whether you believe it is an excellent, good, fair, or poor reason for an outside authority want to talk to you. 1 = Excellent, 2 = Good, 3 = Fair, 4 = Poor

Intellectual curiosity about your area of research
To evaluate a research grant you have applied for
To assess issues surrounding an intellectual property case
To be evaluated by an Institutional Review Board (IRB)
To have government regulators evaluate the research as a potential public safety risk
To have law enforcement evaluate the research as a potential public safety risk
To be shared with law enforcement to aid in an ongoing criminal investigation
To be shared with law enforcement to aid in an ongoing terrorism investigation
To be evaluated by an Institutional Biosafety Committee (IBC)
To have law enforcement evaluate if the research is a potential target of theft of foreign intelligence agencies

Question 5. Now you are going to see some pairs of statements about working with (SPLIT A - Law enforcement officers, SPLIT B - FBI Agents) who sometimes need to talk with scientists in the course of their duties. After reading each pair of statements, please indicate whether the FIRST statement or the SECOND statement comes closer to your own view, even if neither is exactly right. 1 = FIRST statement STRONGLY, 2 = FIRST statement NOT SO STRONGLY, 3 = SECOND statement NOT SO STRONGLY, 4 = SECOND statement STRONGLY. I trust them OR I am suspicious of them

I believe that they are on my side OR I believe they are working against me
They understand my work OR They don't understand my work
They work well with the science community OR They do not work well with the science community
They are primarily interested in the scientific value of my work OR They are primarily interested in restricting my work for security purposes
Scientists working closely with law enforcement agents is good for the scientific community OR Scientists working closely with law enforcement agents is bad for the scientific community
Some science needs to be kept under tight security and not released to the public for safety or security reasons OR All science should be made open to the public once it is ready for publication
More security equals more censorship OR More security does not equal more censorship

Question 6. There are many reasons that (SPLIT A - a law enforcement officer, SPLIT B - an FBI agent) might want to talk with a scientist. For each of the following, please indicate whether you believe it is an excellent, good, fair, or poor reason for (SPLIT A - a law enforcement officer, SPLIT B - an FBI agent) to approach a scientist. 1 = Excellent, 2 = Good, 3 = Fair, 4 = Poor

To clarify the nature of the scientist's research
For the evaluation of the scientist's research as a potential public health risk
To assess intellectual property rights issues related to the scientist's research
To aid in an ongoing criminal investigation
To aid in an ongoing terrorism investigation
To request technical expertise in a particular area of science or technology
To interview the scientist because they are listed as the sponsor of a foreign student or researcher
To evaluate if a scientist's work has possible alternate applications that might constitute a security risk, sometimes called "dual-use" research
To help safeguard it from theft by potential terrorists
To inquire about the activities of one of your colleagues that is an American citizen
To inquire about the activities of one of your colleagues that is not an American citizen
For the evaluation of the scientist's research as a potential national security risk

TABLE 1 (continued)

Complete list of questions asked in the survey

Question 7. Suppose you received a message that a (SPLIT A - Law enforcement officer, SPLIT B - FBI agent) wanted to speak with you in your capacity as a scientist. For many people, this might raise some concerns about why the (LE officer/Agent) would want to contact them. Please indicate how concerned would you be that the (LE officer/Agent) would... 1 = Very concerned, 2 = Somewhat concerned, 3 = Not too concerned, 4 = Not at all concerned.

Read your personal emails
Ask you to monitor the activities of one of your colleagues
Investigate immigration issues related to you or one of your colleagues
Interfere with you conducting your research
Misinterpret your research as a potential public safety risk
Misinterpret your international travel as evidence of illegal activities
Stop you from publishing your research
Interfere with your research funding
Embarrass you in the eyes of your colleagues

Question 8. If you saw something suspicious happening in your workplace that made you concerned about a potential threat to public safety, who would you feel comfortable reporting to?

Your department head	A federal law enforcement officer
Your immediate supervisor	A local law enforcement officer
An institutional safety committee	A state law enforcement officer
Public safety/security officer affiliated with your institution	An institutional review board
Other (Specify)	

Question 9. Have you or any of your colleagues ever been approached by (SPLIT A - a member of law enforcement, SPLIT B - an FBI agent) to discuss something related to your work as a scientist? If yes, Please describe the circumstances under which you were approached by (SPLIT A - a member of law enforcement, SPLIT B - an FBI agent) to discuss something related to your work as a scientist.

Question 10. What is the best way for (SPLIT A - Law enforcement officers, SPLIT B - FBI Agents) to contact a scientist?

Question 11. What could (SPLIT A - a member of law enforcement, SPLIT B - an FBI agent) do to improve relations with the scientific community?

Question 12. What could scientists do to improve relations with the (SPLIT A - law enforcement community, SPLIT B - the FBI)?

Question 13. What is your gender?	
Male	Female

Question 14. In what year were you born?

Question 15. Which of the following best describes the current stage of your career?

Undergraduate	Laboratory technician
Graduate student	Academic staff scientist
Post doctorate	Lab manager
Primary investigator	Retired
Industry scientist	

Question 16. Please indicate how often you work with foreign nationals in your capacity as a scientist.

Often	Never
Sometimes	I am a foreign national
Rarely	

Question 17. Please indicate the highest biosafety level (BSL) work environment you have worked in.

BSL1	BSL4
BSL2	I have never worked in a facility with biosafety levels
BSL3	I don't know

Question 18. Please indicate which of the following materials you work with in your capacity as a scientist:

Animals	Explosive, corrosive, or otherwise toxic chemicals
Viruses	Radioactive isotopes
Bacteria	Select agents
Fungi	Nuclear material
Human subjects	None of the above

Question 19. Please mark the category that best describes the sector you are employed in as a scientist.

Academic	Military
Government, but not military	Private sector

Question 20. Please indicate the level of security in your current workplace.

High (Military level security)
Medium (Secure facility, picture ID required for access, armed guards)
Low (Restricted access to facility, some security personnel presence)
Minimal (Basic locks on doors, no restricted access to facility)



Inspection Reconstruction Project

Assistant Inspectors

Inspection Division

Inspection Reconstruction Project

- Prior emphasis on Field Offices
 - Fixed Schedule
- New focus – Risk Based
 - National Program Reviews
 - Risk Based Field Office and Legat Inspections

b6
b7C

National Program Reviews

- Entire Program - National Perspective
 - 3-Phase/120 Day Process
 - Top Down
 - Observations/Recommendations

National Program Review

- Phase I
 - Broad overview of program

b7E

Broad Overview

- The program is first evaluated at the macro level via a two-week examination of [redacted]
- The evaluation utilizes specific [redacted] have been approved by the substantive division at FBIHQ.

Surveys

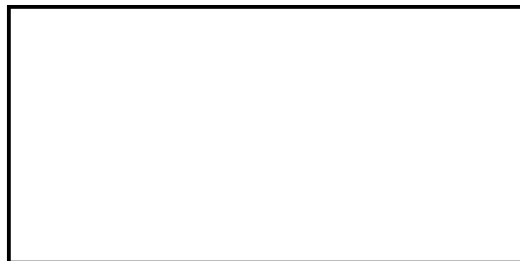
- Climate and Leadership Surveys for substantive division managers are compiled and analyzed by IAU.
- The analysis is provided only to the Inspector in Charge.
- Leadership assessed as High, Medium, or Low.

b7E

Additional Surveys

- Based upon the initial overview, program employee surveys are designed:
 - Field employees working in the program
 - FBIHQ employees

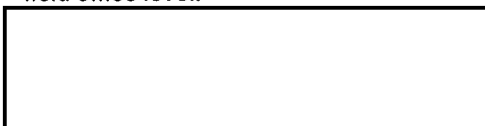
Focused Review



b7E

Focused Review

- A “granular” view of the program at the field office level.



Phase II – HQ Interviews

- Conduct interviews at FBIHQ



b7E

Phase III – On-site Review

- On-site reviews of the relevant program in



Inspector's Report

- At the conclusion of the program review, in depth analysis is completed.
- A report is prepared and provided to the



b7E

Risk Based Field Office and Legat Inspections

- SAPR 2.0 is the cornerstone.
 - Fully automated data.
- Completed each July to cover the period Oct 1 – Jun 30.
 - Current Buded 7/27/2009.
- In late Summer, each substantive division will grade the SAPRs for all Field Offices / Legats.

The SAPR

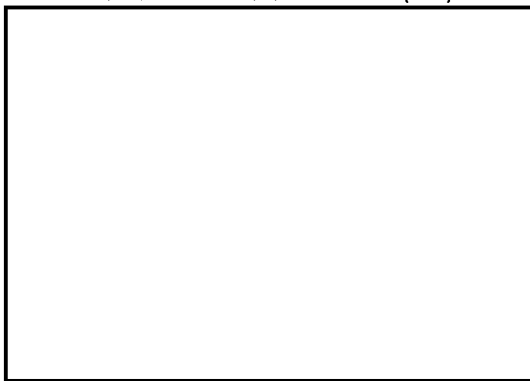
- Eleven Dimensions of Investigative Program:



Impact

b7E

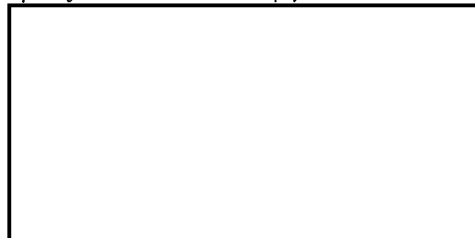
INSPECTION RISK ASSESSMENT MATRIX (IRAM)



SAC EPPA REVIEW: Background

At the request of Deputy Director Pistole, on September 2, 2008, the Inspection Division launched a 30 day review of the existing mechanisms for evaluating SAC performance.

The specific goals of the "SAC EPPA Review" project were as follows:

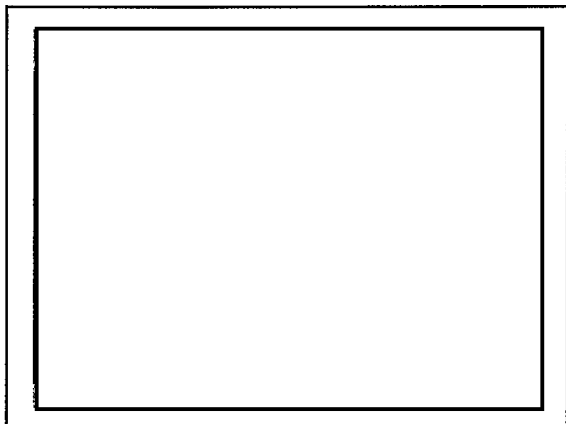


b7E

Summary Composition



b7E



EPPA Workflow Process (Aug-Oct)

- Phase I - Ratings for EPPA components developed by 9/11
- Phase II -
- Phase III -
- Phase IV -
- Phase V -
- Phase VI -

b6
b7C
b7E



Legat Program Team Leader

TL

b6
b7C

Questions and Comments



Inspection Reconstruction Project

Inspector

Inspection Division

b6
b7C



**FBI Laboratory Division
Operational Response Section
Hazardous Materials Response Units**




Unclassified/For Official Use Only

**FBI Hazardous Materials
Response Program**

Established in 1996





3 Operational Units in the Laboratory Division
Operational Response Section:
Hazardous Materials Response Team Unit (HMRTU)
Hazardous Materials Operations Unit (HMOU)
Hazardous Materials Science Response Unit (HMSRU)

Unclassified/For Official Use Only

Mission

- Provide technical, scientific, crime scene and safety response support to FBI investigations involving Hazardous Materials
- Established by USG policy as primary USG civilian response team for:

- Intelligence/Sensitive Site Exploitation Missions in support of FBI Operations

Unclassified/For Official Use Only

Concept of Operation





The HazMat Response Program combines:
FBI Supervisory Special Agents
Career Professional CBRN Scientists
Career Professional Operational HazMat Officers

b6
b7C



Hazardous Materials Response Teams Unit
Hazardous Materials Science Response Unit
Hazardous Materials Operations Unit

Supervisory Special Agents, HazMat Officers, HazMat Specialists, Paramedics, Scientists and Field HMRT Personnel

Established in 1996

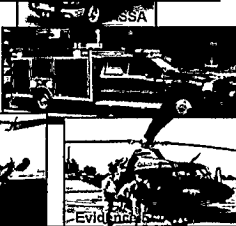


C/Y 2007

Unclassified/For Official Use Only

Response Strategy



Bureau Air

Unclassified/For Official Use Only

b7E

Mission Trends

► July 1996 – May 2007

- Operational Deployments








International Operations



Others

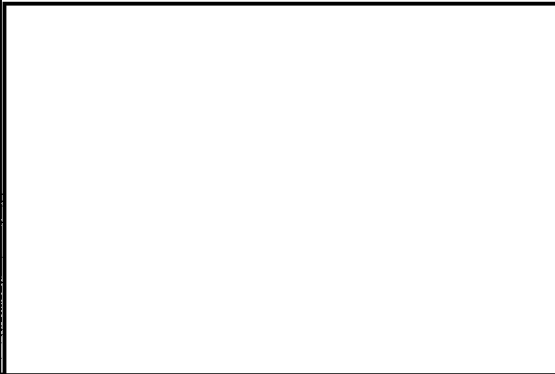


b7D
b7E

Operational Mission Examples



Special Event Mission Examples



b7E

Hazardous Materials Response Teams Unit



► Unit Chief

- Regional WMD Program Management
- Hazardous Materials Response Teams
- Operational Site Management
- Crime Scene and Forensic Training
- National WMD Operational Policy




Unclassified For Official Use Only

HAZARDOUS MATERIALS RESPONSE TEAMS



Unclassified For Official Use Only

b6
b7C
b7E

Hazardous Materials Science Response Unit

- ▶ Unit Chief Dr. [REDACTED]
- Operational Scientists to support FBI WMD missions
- WMD Scientific Evaluations
- WMD Evidence Collection protocols, plans and operations
- National Policy
- Laboratory Response Network Training
 - ▶ Chemistry
 - ▶ Radiological Crime Scene
 - ▶ Microbiology

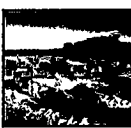





Unclassified/For Official Use Only

Hazardous Materials Operations Unit

- ▶ A/Unit Chief [REDACTED]
- Operational Safety
- Escort Operations
- HazMat Paramedic Program
- Communications/Logistics
- HazMat Robot Program
- Technical Operations
 - ▶ Confined Space
 - ▶ Trench
 - ▶ Joint Hazard Assessment Teams for Special Events
 - ▶ Safety Officer Support
 - ▶ High Hazard Crime Scenes
 - ▶ WMD Tactical Operations
 - ▶ WMD/EOD RSP Operations
 - ▶ OSHA Training
 - ▶ Operations
 - ▶ Technician

Evidence Access Safety Operations




Confined Space Ops Tactical WMD Support

Unclassified/For Official Use Only

b6
b7C

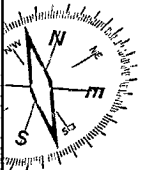
Special Operations

- ▶ Deep Confined Space missions
- ▶ Confined space and rope
- ▶ Pneumatic shoring & trench operations
- ▶ Hydraulic and gas cutting systems
- ▶ Air bag lifting systems
- ▶ Structural shoring
- ▶ Utility Control
- ▶ Listening devices and cameras




Unclassified/For Official Use Only

Risk Based Response



What is reasonable and appropriate?

Unclassified/For Official Use Only

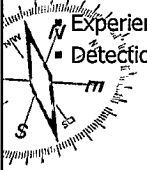
Inherent Conflict



Unclassified/For Official Use Only

Risk Based Response

- ▶ A consensus opinion on protective levels
- ▶ Based upon:
 - Intelligence
 - Observation
 - Experience
 - Detection & Monitoring

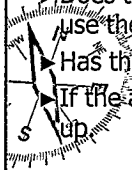


Unclassified/For Official Use Only

b7E

Intelligence

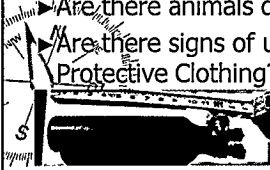
- ▶ Does the Subject have access to materials?
- ▶ Does the Subject have the knowledge to use the materials?
- ▶ Does the Subject have behavioral profile to use the materials?
- ▶ Has the Subject used the materials before?
- ▶ If the answer is yes to any, the risk goes up.



Unclassified For Official Use Only

Observation

- ▶ Are there any containers visible?
 - What type (Solid, liquid, or gas storage)
- ▶ Are there any visual, audible, or olfactory clues?
- ▶ Are there animals dead/alive in the area?
- ▶ Are there signs of use of Personal Protective Clothing?



Unclassified For Official Use Only

Experience

- ▶ Need personnel experienced in Hazmat & Science
- ▶ Can compile Intelligence and Observation components to give a realistic threat level
- ▶ Able to identify potential risks based on observations
- ▶ Able to interpret readings from Detection & Monitoring equipment



Unclassified For Official Use Only

HazMat Program Support to CI Cases

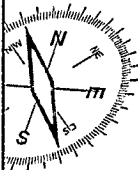
"What can we do for you?"



b7E



b7E



Case Histories

Santa Claus is Coming to Town

► Situation

- Numerous residences during the Amerithrax investigation needed to be covertly searched.
- Great public interest and panic
- Threat of exposure to *Bacillus anthracis*



Unclassified For Official Use Only

"Santa" Technique

► All PPE and Detection and Monitoring in bag

► Respirator donned at door

► Remainder of PPE inside door

► Reverse at exit



Unclassified For Official Use Only

Others

► Vehicles

► Residences

- St. Paul, MN
- Chester, PA

► Other locations

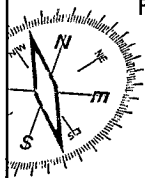


Unclassified For Official Use Only

b7E

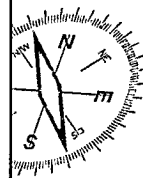


Hazardous Materials Science Response Unit



Federal Bureau of Investigation
Laboratory Division
Operational Response Section

Unclassified For Official Use Only



Unclassified For Official Use Only

b6
b7C

FBI LABORATORY DIVISION
Operational Response Section



FBI LABORATORY DIVISION
Operational Response Section

b7E

~~SECRET~~

~~SECRET//NOFORN~~

National Counterintelligence Program What You Need To Know

Counterintelligence Division

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

What You Need to Know

- FBI's National Strategy for CI 2007-2010
 - CD Strategy Management System (SMS) Map
 - CD SMS Measures
 - CI Program Operations Plan 2008-2009
 - CI [REDACTED] Threat Program Guide
 - CI Strategic Resource & Performance Analysis
- ~~SECRET//NOFORN~~

b7E

~~SECRET//NOFORN~~

FBI's National Strategy for CI 2007-2010

- Issues
 - Counterproliferation
 - Counterespionage
 - Protection of [REDACTED] Assets

(S)

~~SECRET//NOFORN~~

CD Strategy Management System Map

b1
b7D
b7E

~~SECRET//NOFORN~~

CD SMS Measures

- Some of the CD SMS Measures are a direct reflection of programmatic activity at the field office-level
 - Example One - # of distinct CI gaps addressed through analytical products (P6.a)

[REDACTED]

- Example Four - % of Special Agent CI workforce who are rated Proficient (T2.a)
- ~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

Example One - # of distinct CI gaps addressed through analytical products

b1
b7E

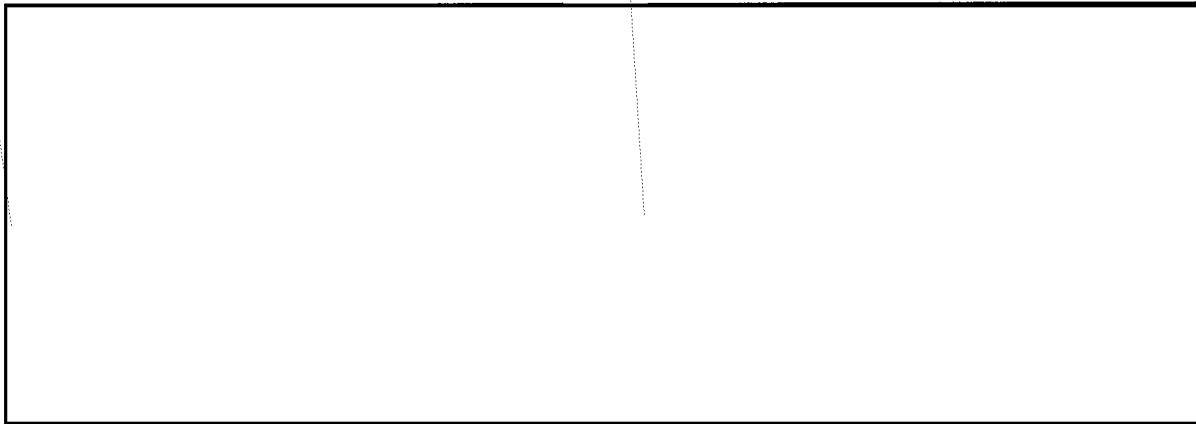
~~SECRET~~

~~SECRET~~

7/13/2011

(S)

(S)



b1
b7E

~~SECRET//NOFORN~~
Example Four - % of Special Agent CI Workforce Who are Rated Proficient

% of CI Special Agent workforce who are rated proficient					
FY 2006	FY 2007	FY 2008	FY 2009 YTD	FY 2009 Target	

(S)

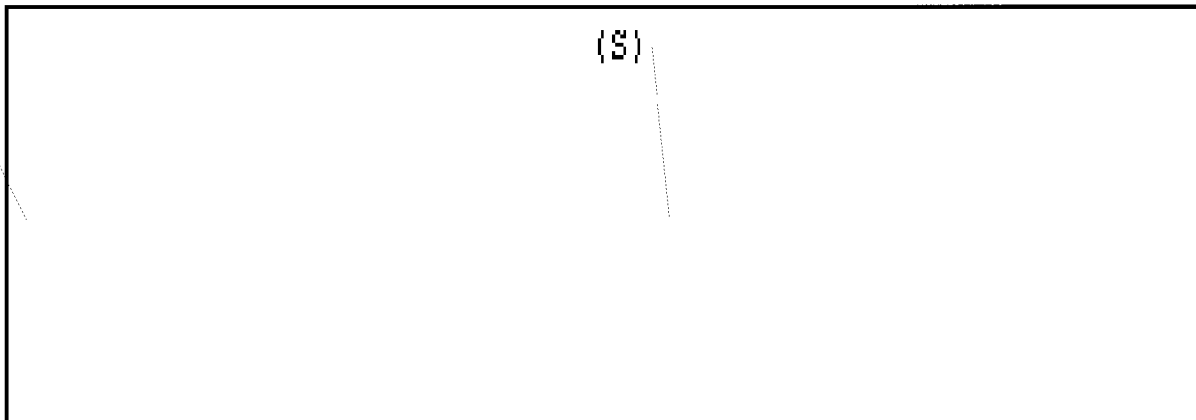
~~SECRET//NOFORN~~
CI Program Operations Plan 2008-2009

- The Counterintelligence Program Operations Plan for 2008-2009 focuses on the priority issues and countries of the FBI's National Strategy for CI and sets out courses of action for CD and field offices.
- The Operations Plan identifies overriding threats, delineates core questions or gaps in our knowledge, and issues targeting directions.
- It de-conflicts guidance that would otherwise be provided individually to the field by each of the CD operational sections.

b1
b7E

(S)

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

(S)



~~SECRET//NOFORN~~
CI Strategic Resource & Performance Analysis

- CD has been reviewing the alignment of CI resources to CI strategic priorities since mid-FY 2007.
- Recently, CD has begun to review the alignment of CI FD-542 statistical data to CI strategic priorities, with the intent to compare with the resource alignment as a measure of performance-based budgeting.
- CD has also begun to review the alignment of both CI resources and FD-542 statistical data to CI [redacted] threats.
- All of these initiatives are measures of performance and rely upon the CI classification structure.
- Therefore, when field office personnel are TURKing, expending resources, and/or claiming FD-542 statistics, it is critical to be comprehensive and accurate when selecting CI classifications and statistical categories.

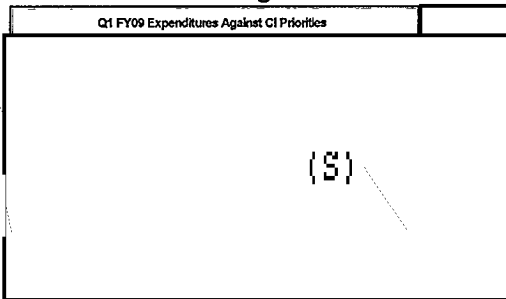
(S)

b1
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
Example of CI Resources Aligned to CI Strategic Priorities

Q1 FY09 Expenditures Against CI Priorities



(S)

(S)

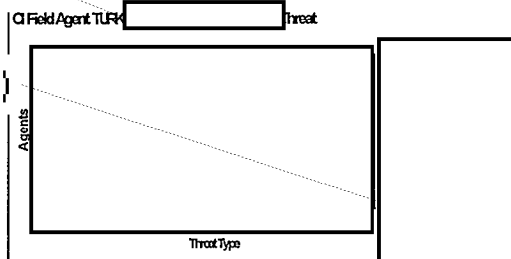
(S)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
Example of CI Field Agent TURK Aligned

(S)

(S)



b1
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~
Contacts

- [redacted] SC J. Chris Woiwode, 202-324-1714
 - FBI's National Strategy for CI 2007-2010
 - CI Program Operations Plan 2008-2009
 - CI [redacted] Threat Program Guide
- [redacted] A/ASC [redacted]
 - CD SMS Map, Measures
 - CI Strategic Resource & Performance Analysis

b6
b7C
b7E

~~SECRET//NOFORN~~

~~SECRET~~

DATE: 02-09-2012

FBI INFO.

/13/2011

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

DECLASSIFY ON: 02-09-2037

~~SECRET~~

SSA [redacted]

Program Manager
[redacted]

Background

First office-Columbia
Drugs and VCMO
CI on newly formed CI squad

Second Office-Atlanta
CI and Domain Coordinator/R5CIWG facilitator

FBIHQ [redacted]

b6
b7C
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Local Working Groups

Where do cases come from?

- From Heaven...Leads from other divisions
[redacted] 105G from
WFO etc)
- From relationships with mutual
stakeholders who have SME and vested
interest in a significant part of the
predicating activity

b7E

Participants

AFOSI
902d
[redacted]
NCIS
[redacted]
Cleared contractors?
Cleared university research administrators
USAO
[redacted]
FBI-all CI bodies

Examples

AFOSI DAOP
[redacted]

b1
b7E

~~SECRET~~

Frequency

What is too often and too seldom?

CO=Quarterly
AT-Monthly

You decide, what is going to make you understand your domain. Then pulse the domain on a regular basis

Some ideas to get started

- Federal Partner (NOT OGAs) Briefing
 - We are _____
 - We are experts at _____
 - _____ keeps us up at night
 - _____ is helpful
 - _____ is not helpful
 - We care about _____
 - We can help the community by _____

Possible Initiatives

- Confucius Institutes
- AIL
- FLO
- Intel gap sub groups

- Tech Task Force

Some more things to consider

- Come up with way points and then move on?
- IDing no threat is okay

No freeloaders

- Share case info when possible with those that have any mutual interest (TT and P and sources excluded)
- Many partners feel their work is not as dynamic as the FBI and are reluctant to share. Big kids share first
- If your squads are participating how does that reflect on the importance to our partners

Regional Counterintelligence Working Groups

7/13/2011

(S)

History

- 10/20/2003. Formation [redacted]
[redacted]
- SACs from each Division
 - FCI Program Manager
 - FCI Program coordinator

[redacted]

(S)

History Continued

- Proposed Agenda
[redacted]
- Partner agency's presentation of:
 - mission, AOR, staffing level

b1
b7E

History (7 months, 20 days later)

- Providing of a TR# for RCIWGs
- Change [redacted] regions
- [redacted] (based on initiatives) part of RCIWGs
- Commerce ((based on initiatives) part of RCIWGs
- Initiative
 - Domain Task Force [redacted]
 - Education/case presentations

Current

[redacted]

- Broader participation
- Closely monitored by CD on SAC Participation for PAR
- SAC/SSA facilitator/SA co-facilitator (new)
- Move the meetings around region to accommodate other constituencies such as [redacted]

b7E

Regional CI Working Groups

[redacted]

Regional CI Working Groups

[redacted]

b6
b7C
b7E

~~SECRET~~

7/13/2011

 FY 2009 Dates and Locations 

--

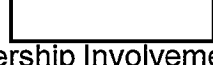
 FY 2010 Dates and Locations 

--

b7E

  Attendance 

Bureau	
Federal Partners	
Non-Federal Partners	

  Leadership Involvement 

--

b7E

 Field Office Participation 

- SAC
- Nat Sec ASAC
- CI SSA
- Intel SSA (or DCM
- Cyber SSA
- Strategic Partnership Coordinator
- Other SME as needed or requested

 HQ participation 

- Program coordinator SSA
- CNA rep SSA/MAPA
- Business Alliance SSA
- Academic Alliance SSA
-  executive member (GS-15 or above)
- 

b7E

~~SECRET~~

~~SECRET~~

7/13/2011



Structure

- Cross Division
- Cross Programmatic
- Cross Agency

Education/Briefings and Working Groups



Bottom Line

- Program Goals and Objectives
- SAPRs
- PARs

- Can we make cases, enhance existing cases and enhance intelligence collections
- No silver bullet
- In CI we have to turn over a lot of rocks, these working groups bring more rocks to turnover

b7E



Questions?

- SSA

 Program Manager

b6
b7C
b7E

~~SECRET~~

~~SECRET~~DECLASSIFIED BY 65179 DMH/STW
ON 02-09-2012

Counterintelligence Training Session September 14, 2009

HRD-ICML
Joint Duty Program Manager



AGENDA

1. Joint Duty policy (three parts) - We have revised the JD policy (published 8/25/09). The policy covers:
 - a. How to claim Joint Duty credit for past assignments (assignment vs leadership training; which will be required at some future date);
 - b. How, as managers, you can post on JWICS for Joint Duty assignments for others in the IC to apply to;
 - c. How a Bureau employee can apply to a JWICS Joint Duty posting.
2. Importance of Joint Duty Credit for YOU.
 1. SES positions that require JD credit.
 2. NSB EC "preferred criteria".
 1. How to file a Joint Duty Claim
 - a. Supporting documentation - See FAQs on JD site "Claim Forms" #9.
3. Latest Update on Joint Duty Program and Database.

b6
b7C
b7E



Policy and importance of JD

1. Newly published policy covers:
 - a. How to claim Joint Duty credit for past assignments (assignment vs leadership training; which will be required at some future date);
 - b. How, as managers, you can post on JWICS for Joint Duty assignments for others in the IC to apply to;
 - c. How a Bureau employee can apply to a JWICS Joint Duty posting.
2. Importance of Joint Duty Credit for YOU.
 1. SES positions that require JD credit. JD policy states all NSB SES, ADIC and NSB SACs under ADIC offices must have credit in phased in approach
 2. NSB EC "preferred criteria" - NSB published EC that JD is a preferred criteria for GS-14 and GS-15 SSA and IA and some MAPA positions at HQ and the field, so this will be important as you apply to NSB ASAC jobs and NSB HQ jobs in the future.



Internal Assignment Language - found on JD site under FAQs "Claim Forms" #9

9. What documentation do I need to include in support of my claim?
Please include anything you have that proves the following 4 criteria for Joint Duty:

b7E



How to file a claim for JD:
Log on to the system from



Next screen hit Continue and then select the link for

b7E

~~SECRET~~



Where you will see your name and the Menu page, then go to *New Claim*:



Where you see the screen to type in your claim information:

b6
b7C
b7E



After you enter claim information in the system:

Once you enter the claim form it will show up as:

- Submitted
- Pending
- Approved

You will not get hard copies back



Latest Update on JD program and Database

Latest Update on Joint Duty Program and Database:

1. Updated
2. Updated Directive and Policy:
3. Updated manual for employees and Admin and Reports Users to the
4. Detailee OUT conference 9/24 for detailees OUT of FBI in HQ-DC areas.
5. Detailee Link made public for detailees IN and OUT (Found on JD site) of FBI that HQ Admin staff must maintain. This will be required for field in future.

b7E



Questions/Comments?

information:

Unclass email:

Hi side email:

email box:

b6
b7C

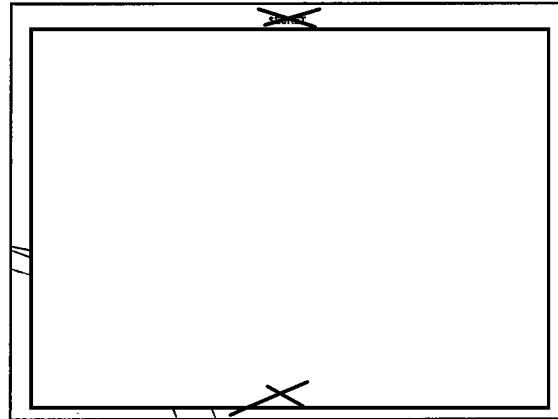
DATE: 02-14-2012

CLASSIFIED BY 65179 DMH/STW

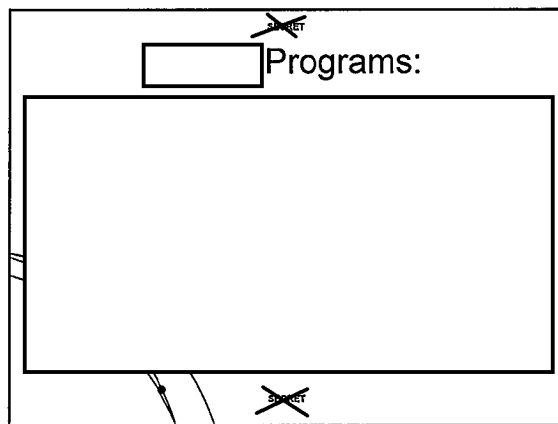
REASON: 1.4 (C)

DECLASSIFY ON: 02-14-2037

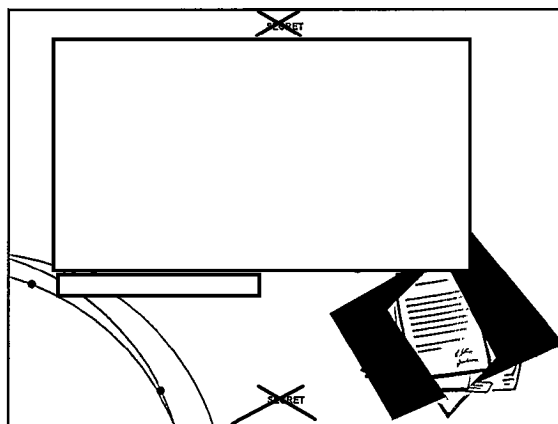
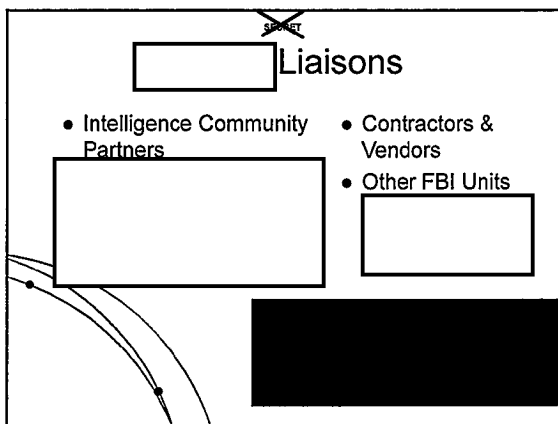
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b7E



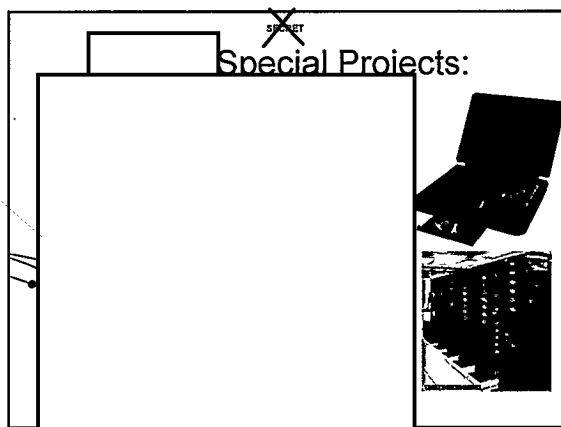
b7E



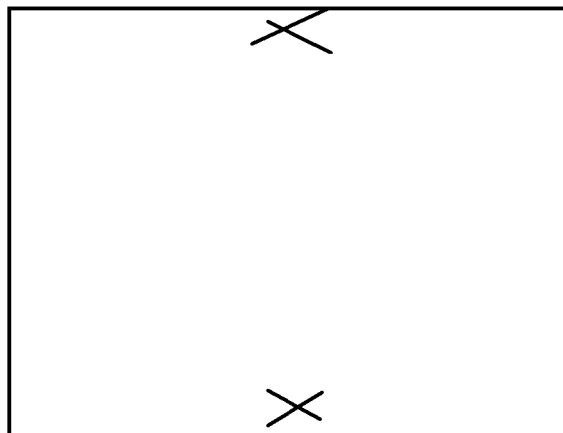
b7E



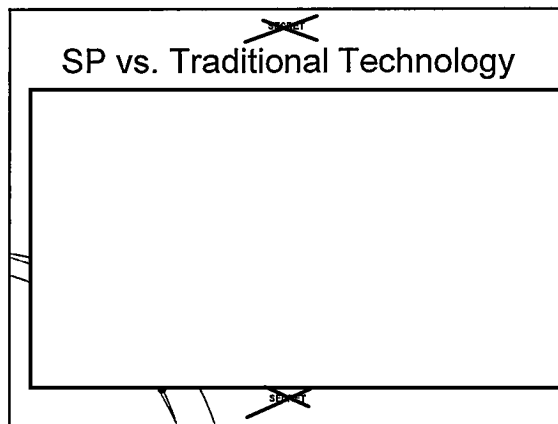
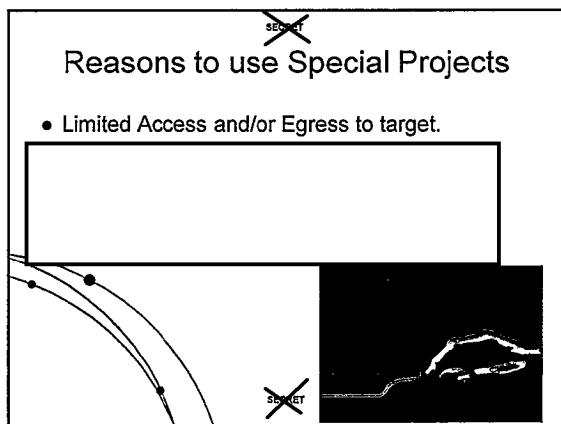
b7E



(S)



b1
b7E



b7E

~~SECRET~~

Special Project Process

- Steps to implement a Special Project
 - Determine need and Coordinate with TTAs.
 - Complete Special Project Request Form(s).
 - EC to delineate the operational need.
 - Blind Faith report.
 - Technical / Operational plan.
 - Special Project Approval Board (SPAB).
 - Other Issues [REDACTED]

~~SECRET~~

[REDACTED] CONTACTS

[(202)324-XXXX]

- UC [REDACTED]
- SSA [REDACTED]
- SSA [REDACTED]
- SSA [REDACTED]
- MAPA [REDACTED]
- MAPA [REDACTED]
- MAPA [REDACTED]

~~SECRET~~

b6
b7C
b7E

Questions?



~~SECRET~~

b7E

~~SECRET~~

~~SECRET~~

7/13/2011

DATE: 02-14-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-14-2037

(S)



(S)

[Redacted] Capabilities Overview

- This presentation lays out a very basic look into the disciplines and capabilities that make up the [Redacted] [Redacted] it will define the Operational Technology Division's various roles and define how Technology aids intelligence gathering initiatives, investigations and helps meet collection requirements and fills intelligence reporting gaps.
- At the end of the presentation, the audience will have a raised awareness of additional avenues they can employ in their identified collection strategies as well as how to seek out these resources.

b1
b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

What is the Operational Technology Division?

- The FBI's Operational Technology Division is one of the cornerstones of the FBI's Science & Technology Branch.
- Headquartered on [Redacted]

What is the Operational Technology Division?

- OTD is currently structured into 5 distinct Sections:

[Redacted]

b7E

What is the Operational Technology Division?

- Responsible for the "Meat and Potatoes" of what you generally think of when you envision Technical Intercepts.

[Redacted]

- OTD's analytical cadre: the Technical Evaluation Office (TEO)

What is the Operational Technology Division?

- Provides technologies that enable collections of communications from a Service Provider point of intercept.

(S) [Redacted]

(S) Also includes [Redacted]

(S) [Redacted]

b1
b7E

~~SECRET~~

What is the Operational Technology Division?

[Redacted]

- These are the "Entry Teams"
- Are composed of several Tactical Operations Units (TACOPS) that are very specialized and include:

[Redacted]

(S)

What is the Operational Technology Division?

[Redacted]

b1
b7E

What is the Operational Technology Division?

[Redacted]

- Management of Field Technical Resources, both offensive and defensive. (TTA's and ET Programs)
- Management or Technical Training and Certification Programs
- Technical Response Capabilities for Emergency or Special Event scenarios
- Aggressive technical industry liaison and outreach programs.

What are the Capabilities?

- From the 50,000 foot view.

[Redacted]

b7E

What are the Capabilities?

- From the 20,000 foot view:

[Redacted]

(S)

What are the Capabilities?

- From the 20,000 foot view:

[Redacted]

- Again, Concealment is key

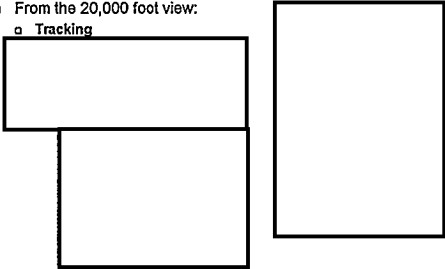
[Redacted]

b1
b7E

What are the Capabilities?

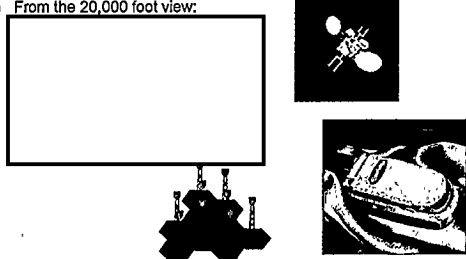
■ From the 20,000 foot view:

- Tracking



What are the Capabilities?

■ From the 20,000 foot view:



b7E

What are the Capabilities?

■ From the 20,000 foot view:

- Data Intercept



(S)

What are the Capabilities?

■ From the 20,000 foot view:



b1
b7E

What are the Capabilities?

■ From the 20,000 foot view:

- Remote Operations



What are the Capabilities?

■ From the 20,000 foot view:

- Surreptitious Entry



b7E

7/13/2011

What are the Capabilities?

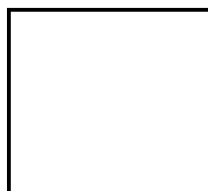
- From the 20,000 foot view:



(S)

What are the Capabilities?

- From the 20,000 foot view:
 - Technical Analysis

b1
b7E

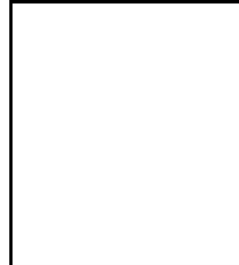
What are the Capabilities?

- From the 20,000 foot view:
 - Analytical Evaluation



What are the Capabilities?

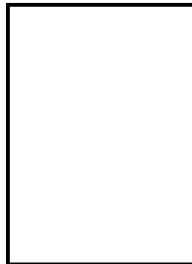
- From the 20,000 foot view:



b7E

Technical Operations Notes and Considerations

- Technical Operations are Passive?!?!?

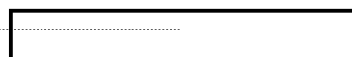


...not!!!

(S)

Technical Operations Notes and Considerations

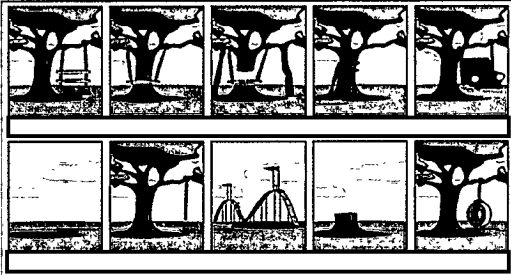
- Technical Sources may be Static, but they are as Passive as you manage them to be.
- Like Human Sources:
 - they take a very dedicated support effort maintain
 - they are manpower intensive
 - some are better than others
 - reporting capability is dependant on analysis of supplied intelligence
 - should be scrutinized on a regular basis

b1
b6
b7C
b7E

~~SECRET~~

7/13/2011

Defining Requirements



Defining Requirements

- Knowing what you need to target is Key to a successful technical source penetration.
 - Work with [redacted]
 - Work with [redacted]
 - Work with [redacted]
 - Work with [redacted]
 - Work with [redacted]
 - Work with [redacted]
 - Work with [redacted]
- Everyone needs to be in the loop.

b7E

Defining Requirements

- Legal and Political Considerations
 - Standard [redacted] Definitions
 - Reference [redacted] Court definitions
 - Special Project Approval Board



Defining Requirements

- Case Examples:
 - Reactive Opportunities
 - Proactive Opportunities

b7E

Mitigating Risk

- Risk Mitigation, ie Risk vs Gain analysis is an integral part of defining requirements.
- Risk analysis is an art unto itself. The Technical Advisor and the TTA cadre coupled with OTD, especially TEO input is crucial to understanding the variables and impacts associated with risk mitigation.
- Experience and training provide the basis for a sound analysis.

Need more additional information about OTD's services?

- Talk to your Technical Advisor or TTA



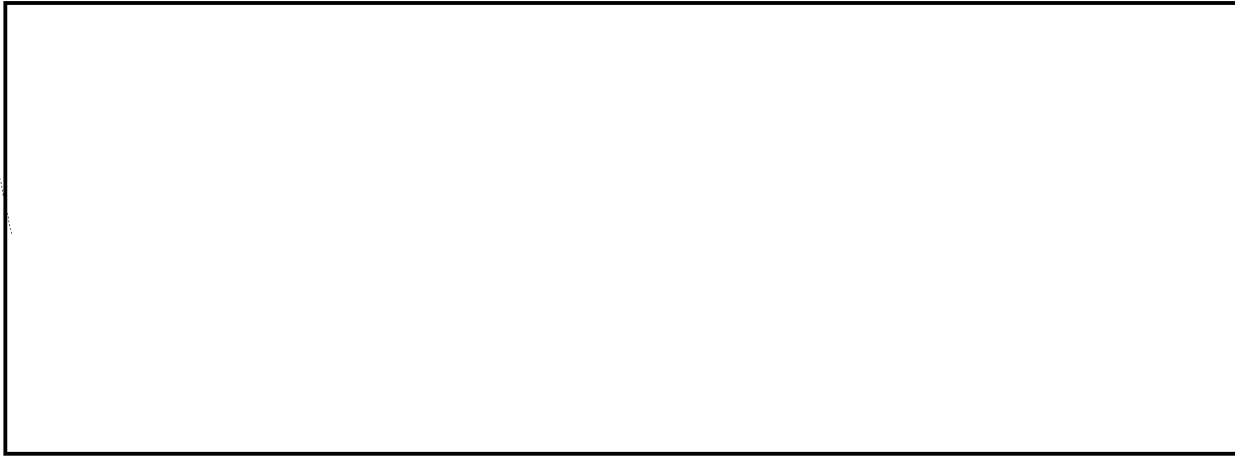
- Contact Technical Operations Coordination Unit for help.
 - Unit Chief [redacted]
 - SSA [redacted]
 - TEO Lead Analyst [redacted]

b6
b7C
b7E

~~SECRET~~

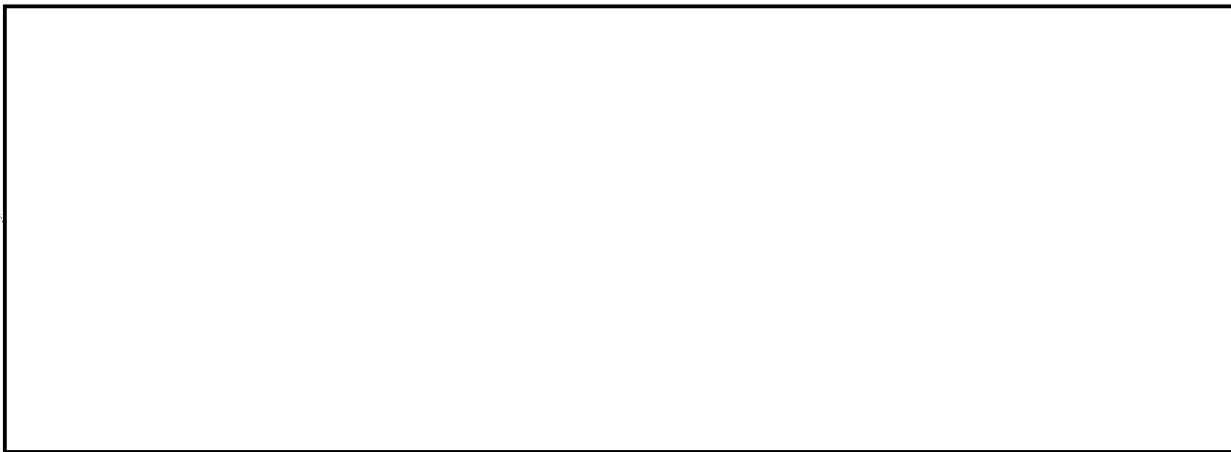
~~SECRET~~

(S)



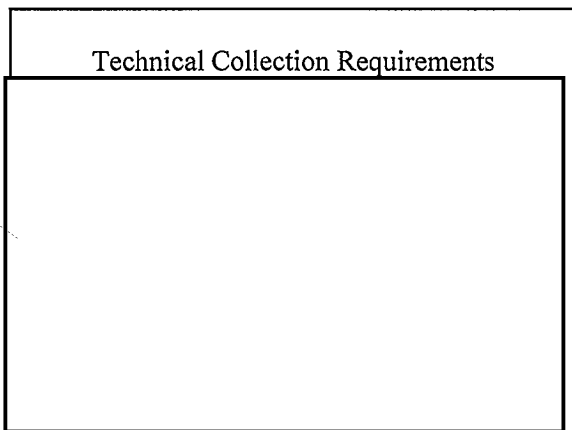
b1
b7A
b7E

(S)



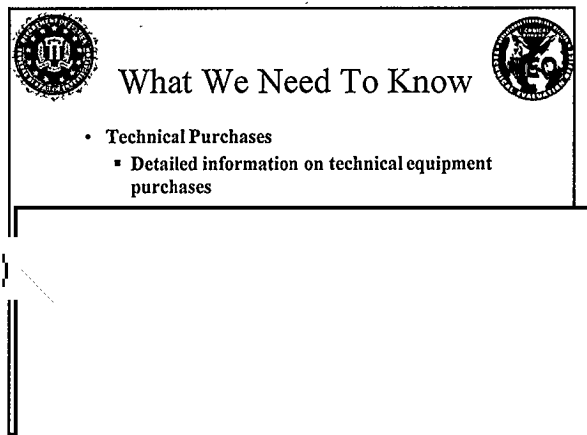
b1
b7D
b7E

(S)



Technical Collection Requirements

(S)



What We Need To Know

- Technical Purchases
 - Detailed information on technical equipment purchases

b1
b7E

~~SECRET~~

~~SECRET~~

Technical Threat Analysis Program

7/13/2011

	Technical Evaluation Office 	
	TEO Program Manager SIA	
	Analysts 	
July 13, 2011	UNCLASSIFIED	25

b6
b7C

~~SECRET~~

~~SECRET/NOFORN~~

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

Foreign Intelligence Activities in the
United States

Acting Section Chief
FBIHQ/CD-1
~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

b1
b6
b7C
b7E

(S)

(S)

Role of the

b1
b7E

(S)

b1
b7E

~~SECRET~~

~~SECRET/NOFORN. Derived from Multiple Sources;
Review for Declassification on 3/8/2031~~

ACLURM043283

(S)

--

b1
b7E

Liaison Relationship

Outside

Activity

(S)

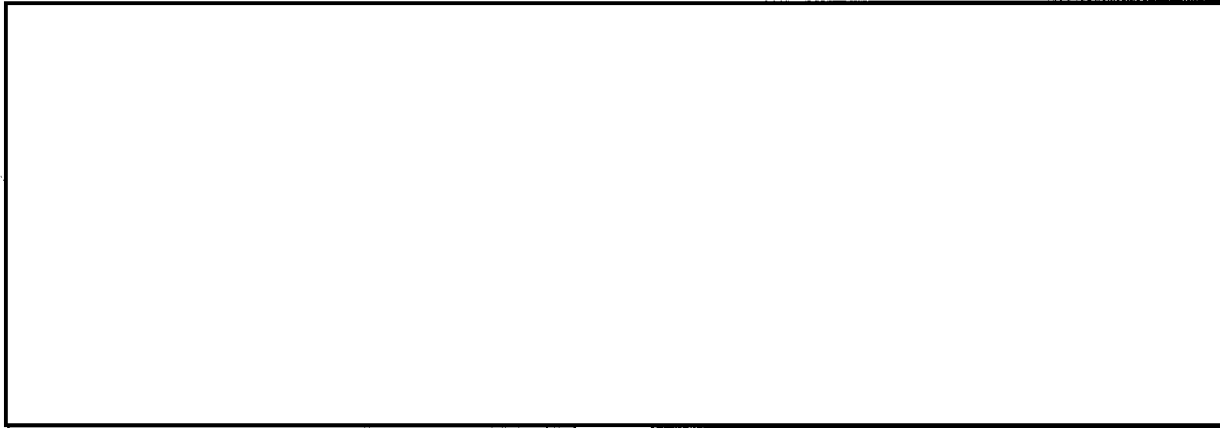
--

b1
b7E

~~SECRET~~

~~SECRET//NOFORN~~

(S)



b1
b7E

Visitors

Visitors

♦ FY2008, 145,725 non-immigrant visas issued

(S)

(S)

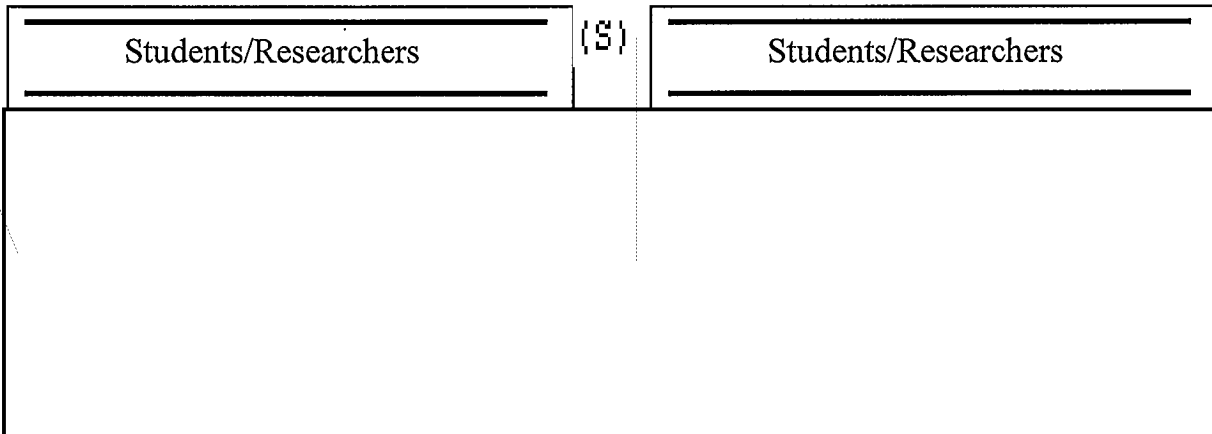
b1
b7D
b7E

Students/Researchers

Students/Researchers

(S)

(S)



b1
b7D
b7E

~~SECRET~~

~~SECRET//NOFORN: Derived from Multiple Sources;
Review for Declassification on 3/8/2031~~

ACLURM043285

Emigres

Emigres

(S)

b1
b7D
b7E

Emigres

Summary

(S)

b1
b7D
b7E

(S)

b1
b7D
b7E

Strategic Partnership Program: A Field Perspective



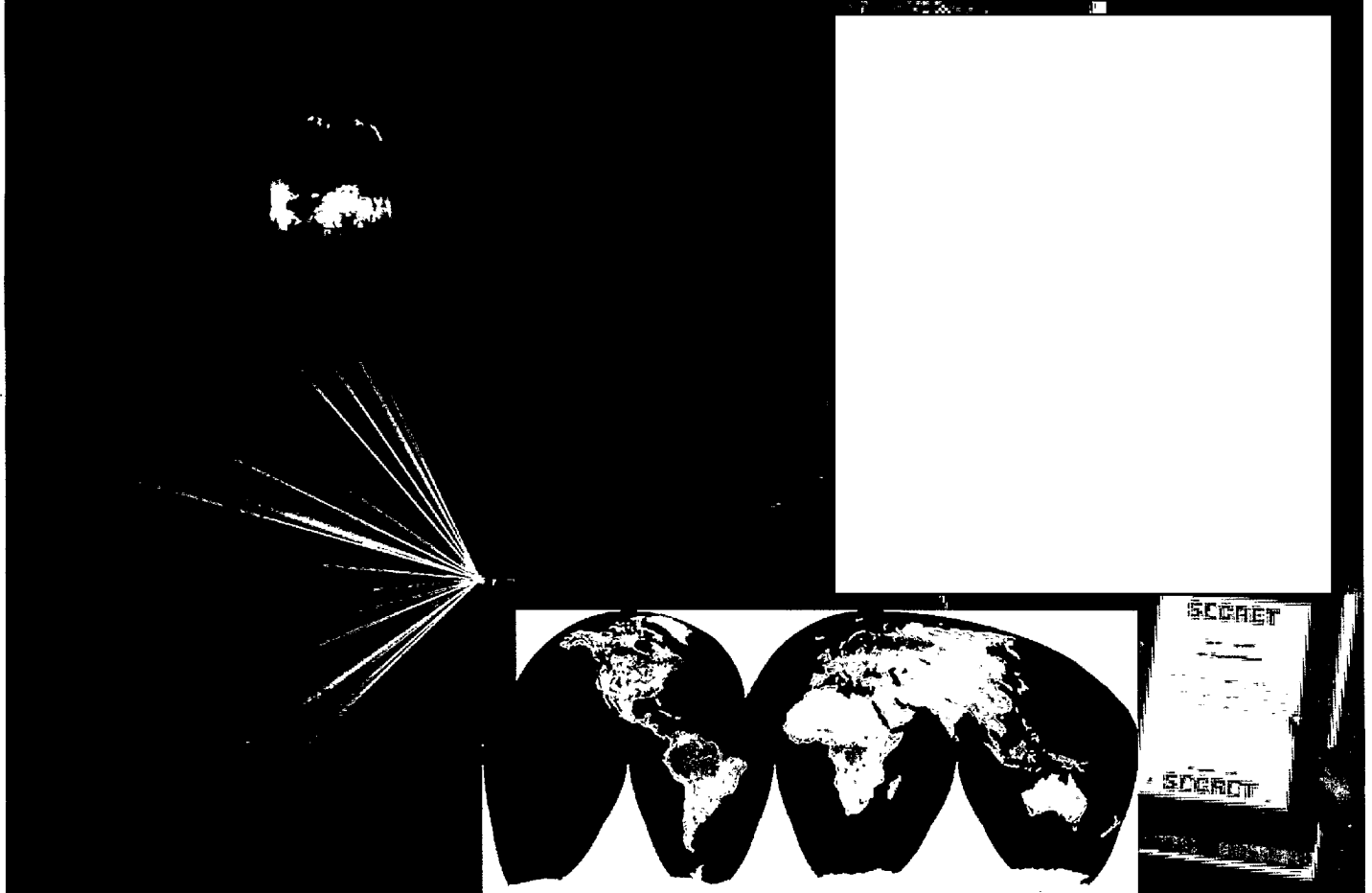
SSA [REDACTED]
FBI-San Francisco

[REDACTED]

b6
b7c

~~SECRET~~

FBI Counterintelligence National Strategy



b6
b7C

~~SECRET~~

~~SECRET~~

Strategic Partnership Program Mission Statement



Generate new, and enhance
existing, investigations and
offensive counterintelligence
operations

Identify new sources

Produce intelligence

~~SECRET~~

~~SECRET~~

(S)

Strategic Partnership Program Focus:



b1
b6
b7C
b7E



~~SECRET~~

~~SECRET~~

Implementing the FBI's Strategic Plan and SPP Mission Statement



CACI
EVER VIGILANT

BAE SYSTEMS

LOCKHEED MARTIN

NORTHROP GRUMMAN
Defending the Future

GENERAL DYNAMICS
Strength On Your Side

ITT

Rolls-Royce

BOEING

L3
communications

Honeywell

United Technologies

Raytheon

SAIC
From Science to Solutions

Booz | Allen | Hamilton

CSC

GE imagination at work



MONTEREY INSTITUTE
OF INTERNATIONAL STUDIES

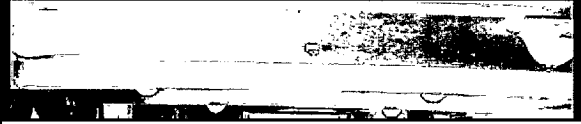
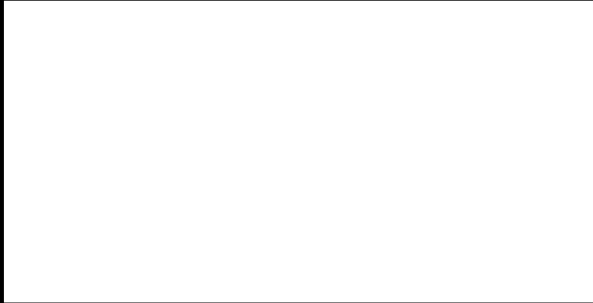


b7E

~~SECRET~~

~~SECRET~~

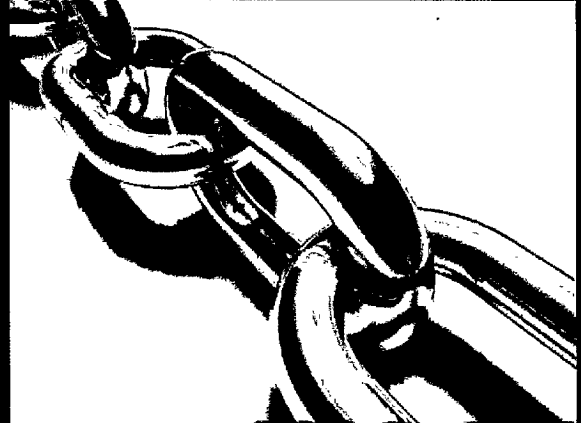
Partnering with USIC



b6
b7C



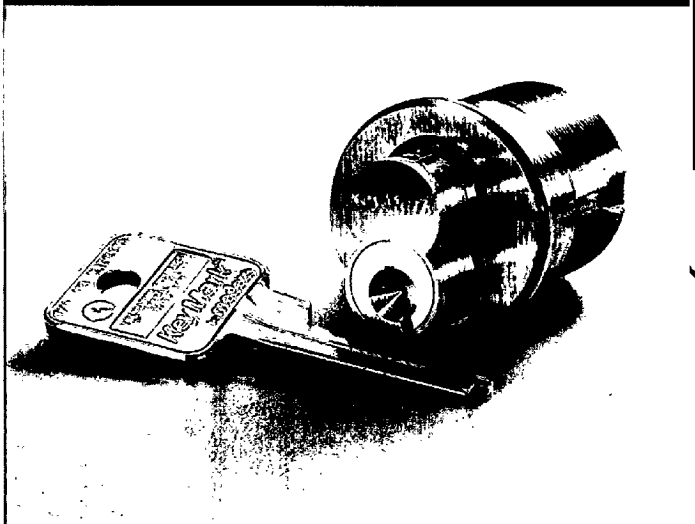
Referrals
Regional Working Groups
Joint operations



~~SECRET~~

~~SECRET~~

Partnering with Business and Academia



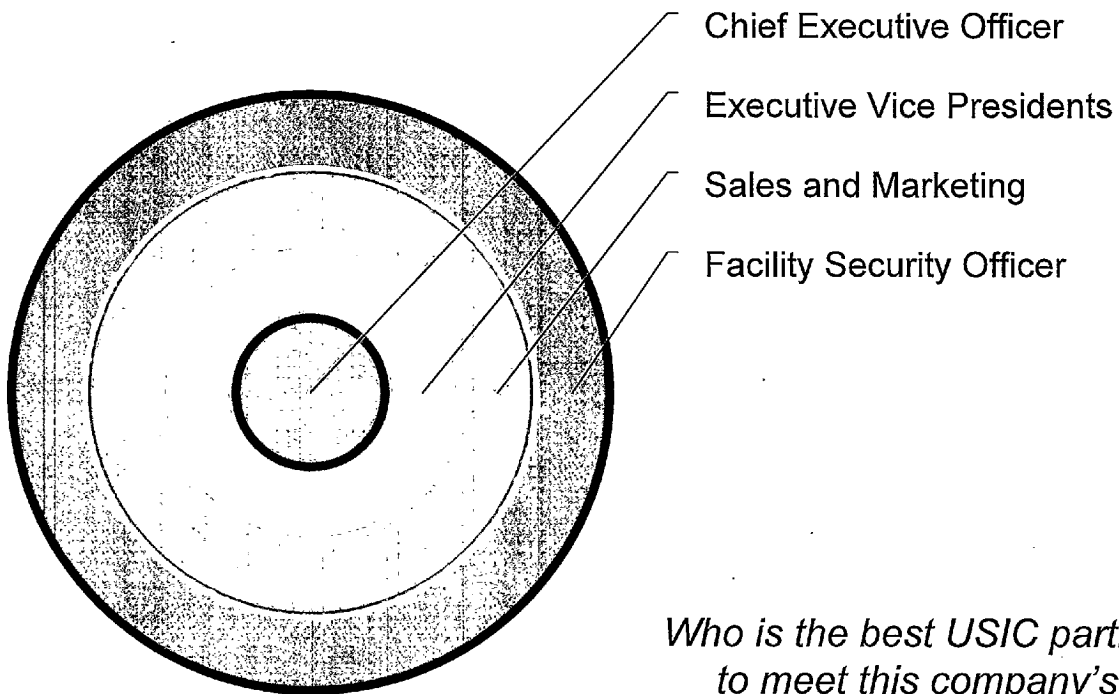
Harden target
Train
Listen

b6
b7C

~~SECRET~~

~~SECRET~~

Counterintelligence SP Briefings: Partnership Methodology

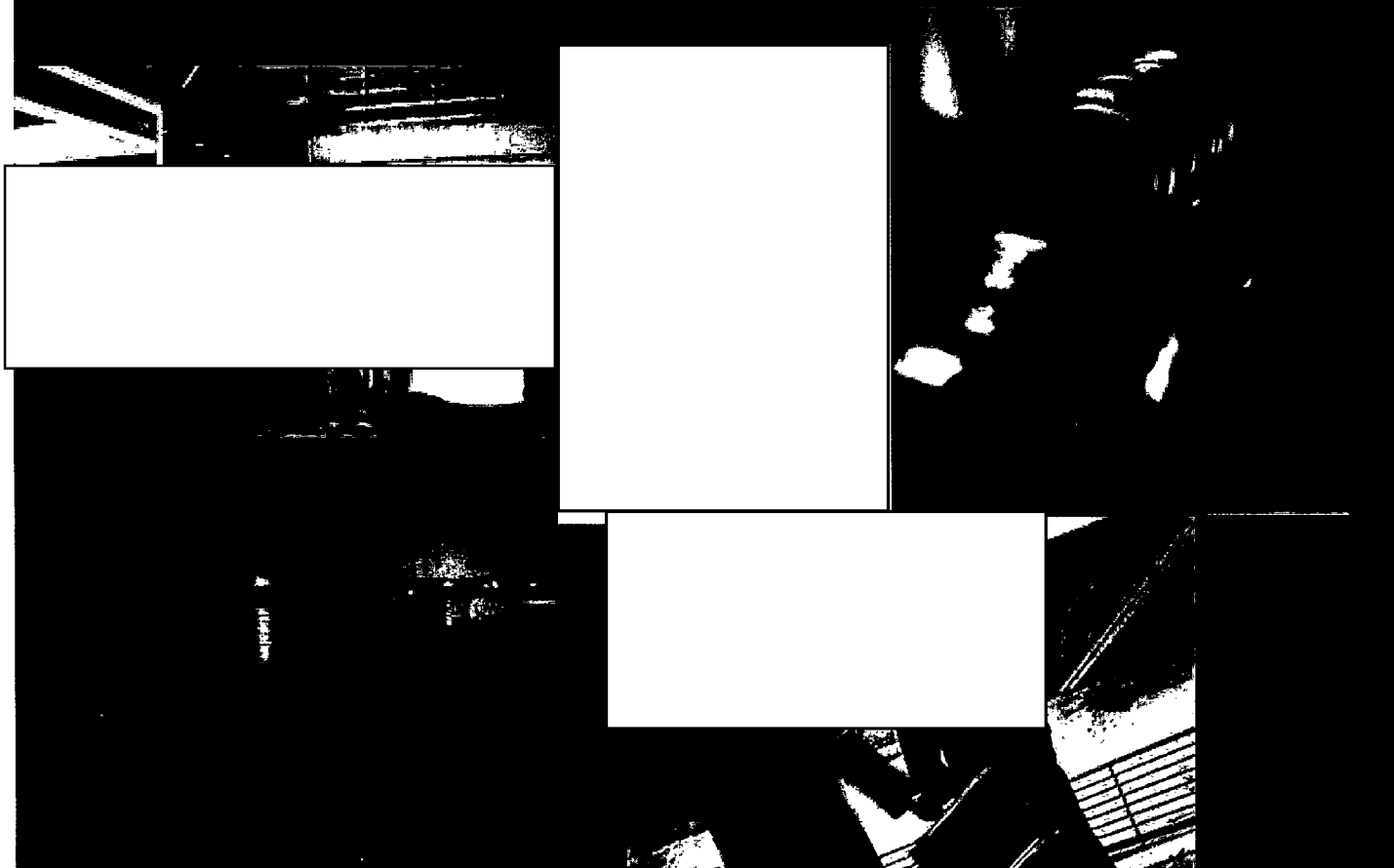


*Who is the best USIC partner
to meet this company's
representative?*

~~SECRET~~

~~SECRET~~

Program Success

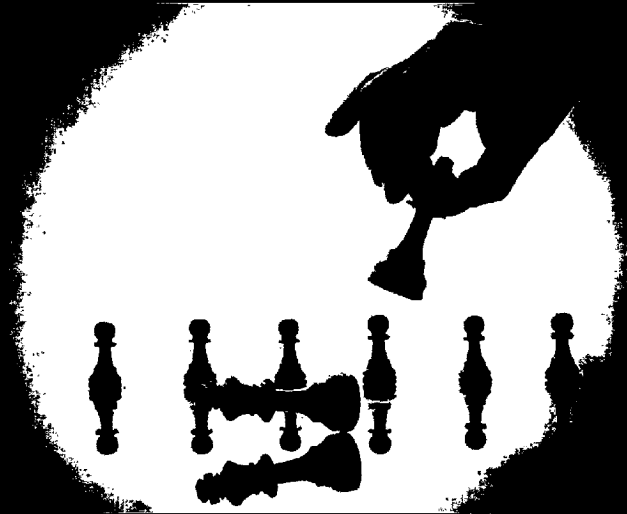
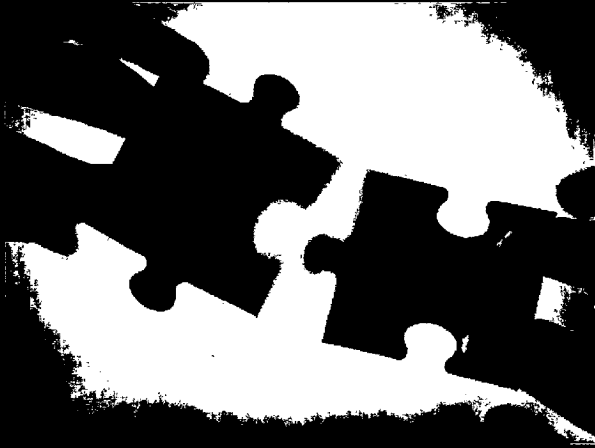


b6
b7C
b7E

~~SECRET~~

~~SECRET~~

Internal Coordination



Analysis
Strategy

~~SECRET~~

~~SECRET~~

Deconfliction

~~SECRET~~

~~SECRET~~

7/13/2011

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~

Federal Bureau of Investigation

Strategic Exploitation Unit

[Redacted]

Driving National Operations Against
Specified Hard Targets

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

SEU Mission: The SEU is a national FBI capability that fuses

[Redacted]

The SEU and its IC partners maintain simultaneous domestic and
international focus

[Redacted]

(S)

b1
b7E

~~SECRET//NOFORN~~

SEU The CI Strategy, SMS and SET

■ FBI CI Strategy

- Directly addresses **STRATEGIC FOCUS**:
 - Protect the United States from foreign intelligence activities.
- By emphasis on specific **PROGRAM ACTIVITY**:
[Redacted]

■ Strategy Management System

- SEU operations directly relate to:
[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

How will the Strategic Exploitation Unit
help my case?

[Redacted]

~~SECRET//NOFORN~~

b6
b7C
b7E

~~SECRET//NOFORN~~

SEU Methodology

- Priority IC/FBI Intel Requirement: With the assistance of
[Redacted]

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

USIC COOPERATION:
Current vs. Proposed

[Redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011

~~SECRET~~

System Criteria/Capabilities

- Enable multi-faced investigations from a criminal and national security vantage

- Robust analytic platform

~~SECRET~~

~~SECRET~~

Use of the Palantir System to Support SEU Operations

- Collaboration: common ontology as the means

- Operations and Targeting Management:

~~SECRET~~

b7E

~~SECRET~~

SEU Target Location Breakdown

Target Office Breakdowns:

- Identifies offices' core competencies
- Personnel allocations per office
- Support services allocations per office

~~SECRET~~

~~SECRET~~

SEU Infrastructure Targeting Matrix

~~SECRET~~

b7E

~~SECRET~~

SEU Operations

(S)

- SEU - IC shaping operations: The SEU can leverage assets

- Field Office / SEU / IC operational action: The SEU will coordinate

~~SECRET~~

~~SECRET~~

Executing the Project

- Phase I - Legal and Resources
 - Solidify Concept of Operations - timeline
 - Identify personnel and funding requirements
- Phase II - Pre-Deployment preparations
 - Develop and refine operational plan
- Phase III - Deployment
- Phase IV - Delivery
 - Data delivery and infrastructure operation and maintenance



~~SECRET~~

b1
b7E

~~SECRET~~

~~SECRET~~

7/13/2011



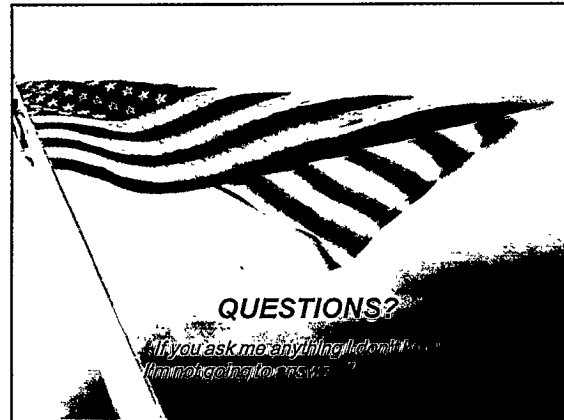
Managing the Collection

- Managing Collection
 - Data to FBI and IC
 - Stay engaged with technical experts
 - Demand/ensure highest quality product
 - Constant coordination
- Pro-active collection operations
 - Tailor collection appropriately



- Constant coordination
- Disseminating Collection
 - Constant coordination

~~SECRET~~



b7E

~~SECRET~~

~~Secret~~

DATE: 02-14-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-14-2037

~~SECRET~~

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

~~SECRET~~ SURVEILLANCE PROGRAM



SPECIAL SURVEILLANCE GROUP

7/13/2011

1

~~SECRET~~ Special Surveillance Group (SSG)

- Mobile component
- 52* Field Divisions
- Investigative Specialist

7/13/2011

2

b1
b7E

~~SECRET~~ SSG Utilization



7/13/2011

3

~~SECRET~~ SSG Organization

- SSA or SA Coordinator

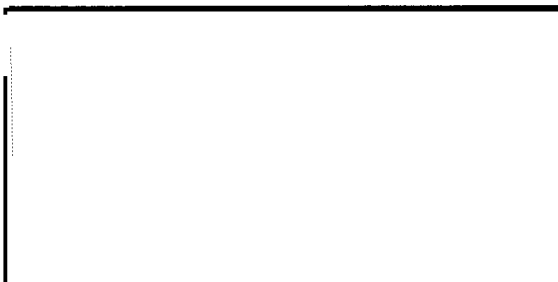


7/13/2011

4

b7E

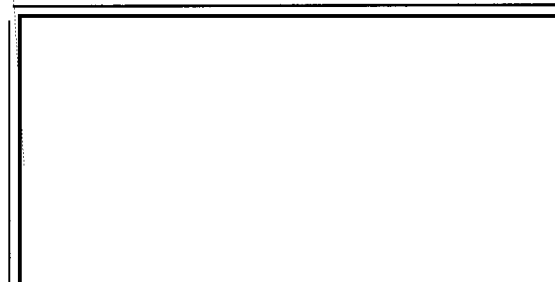
(S)



7/13/2011

5

(S)



7/13/2011

6

b1
b7E

~~SECRET~~

~~Secret~~

ACLURM043301

7/13/2011

(S)

~~SECRET~~

ORGANIZATION

- SSA or SA Coordinator

7/13/2011 7

(S)

~~SECRET~~

Training

- New SSC personnel must complete and pass

7/13/2011 8

b1
b7E

(S)

~~SECRET~~

SURVEILLANCE TDY REQUEST

- Complete SSC surveillance request found on website under forms.
- Prepare a brief ec describing case/goals directed to substantive FBIHQ desk and to the attention of the Physical Surveillance Unit (PSU).
- Appropriate Section Chief must approve request via ec and/or e-mail.
- NO TDY DEPLOYMENTS WILL OCCUR WITHOUT SC APPROVAL!!
- Once approved PSU will provide TR# coordinate teams, and equipment issues.

7/13/2011 9

~~SECRET~~

PHYSICAL SURVEILLANCE UNIT (PSU)

PSU is responsible for providing

7/13/2011 10

b1
b7E

~~SECRET~~

Reorganization

- Move from CD to CIRG official 10/01/2009
- New Surveillance and Aviation Section
- Program Managers and MAPAs provide program management by regions.

7/13/2011 11

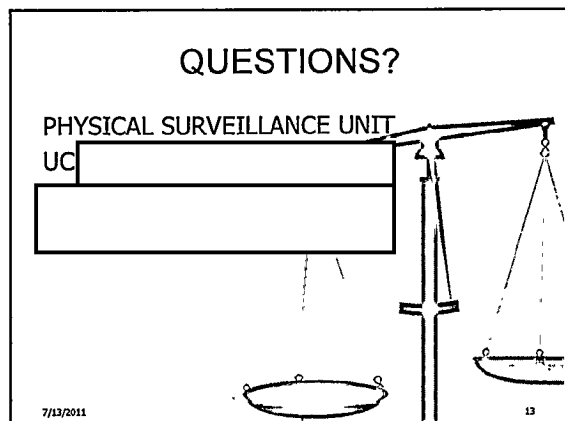
~~SECRET~~

SURVEILLANCE AND AVIATION SECTION

SC
BUTTS KANSAS

7/13/2011 12

b6
b7C
b7E



b6
b7C

DATE: 02-09-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-09-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence Undercover Operations

- [redacted] Clandestine Operations Unit (COU)
- UC [redacted]
- SSA [redacted]

7/13/2011

~~SENSITIVE~~

1

Outline

- I. FBI Undercover Operations (UCOs) - Past and Present
- II. Terms of Reference
- III. Developing UCOs
- IV. Support for UCOs

7/13/2011

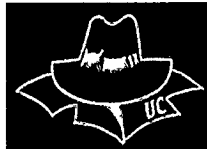
~~SENSITIVE~~

2

b6
b7C
b7E

I. FBI UCOs - Past

- FBI established in 1908
- Earliest documented Undercover Operations in the 1920s in Criminal Investigations



7/13/2011

~~SENSITIVE~~

3

FBI UCOs - Past



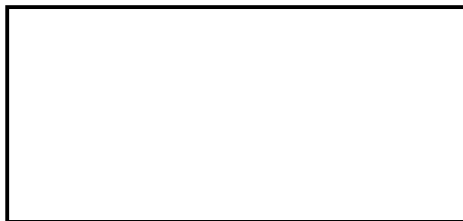
7/13/2011

~~SENSITIVE~~

4

b6
b7C

FBI UCOs - Present



7/13/2011

~~SENSITIVE~~

5

Terms of Reference

- Undercover Employee
 - Any Special Agent, Support Employee, Task Force Agent/Officer, or other person, acting at the behest of the FBI in the conduct of undercover activities.

7/13/2011

~~SENSITIVE~~

6

b7E

~~SECRET~~

ACLURM043304

FBI042204

~~SECRET~~

UCes Today



7/13/2011

~~SENSITIVE~~

7

Terms of Reference

■ Undercover Activities

- Any investigative activity involving the use of an assumed name or cover identity by an Undercover Employee (UCE) for the purpose of concealing the UCE's affiliation with the FBI or USIC during substantive contacts with the target of an FBI investigation. Such activities may include contacts with targets of opportunity when continued contact is not anticipated.

7/13/2011

~~SENSITIVE~~

8

Terms of Reference

■ National Security UCO

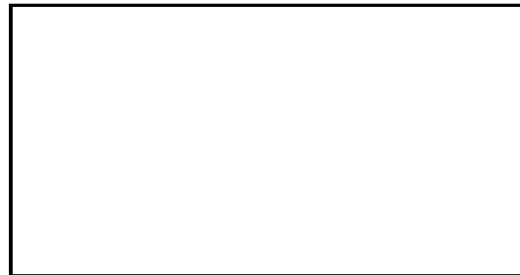
- A series of related undercover activities by a UCE engaging in a relationship with the targets of a foreign counterintelligence or international terrorism investigation where the contact is expected to continue over a period of time and where FBI affiliation is concealed.
 - A "series of contacts" is more than five substantive contacts, contributing information of investigative interest, with the subject (s) under investigation, regardless of the number of UCes making the contacts.

7/13/2011

~~SENSITIVE~~

9

Terms of Reference



7/13/2011

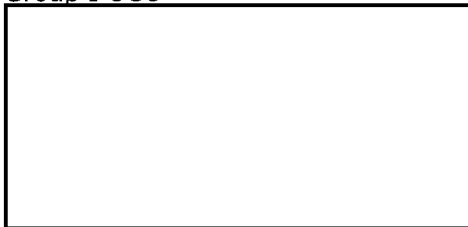
~~SENSITIVE~~

10

b7E

Terms of Reference

■ Group I UCO



7/13/2011

~~SENSITIVE~~

11

Terms of Reference

■ Group II UCO



7/13/2011

~~SENSITIVE~~

12

b7E

~~SECRET~~

Serial Description ~ Unrecorded Serial

Serial	Description	Unrecorded Serial
1	Delet	77
2	Delet	77
3	Delet	77
4	Delet	77
5	Delet	77
6	Delet	77
7	Delet	77
8	Delet	77
9	Delet	77
10	Delet	77
11	Delet	77
12	Delet	77
13	Delet	77
14	Delet	77
15	Delet	77
16	Delet	77
17	Delet	77
18	Delet	77
19	Delet	77
20	Delet	77
21	Delet	77
22	Delet	77
23	Delet	77
24	Delet	77
25	Delet	77
26	Delet	77
27	Delet	77
28	Delet	77
29	Delet	77
30	Delet	77
31	Delet	77
32	Delet	77
33	Delet	77
34	Delet	77
35	Delet	77
36	Delet	77
37	Delet	77
38	Delet	77
39	Delet	77
40	Delet	77
41	Delet	77
42	Delet	77
43	Delet	77
44	Delet	77
45	Delet	77
46	Delet	77
47	Delet	77
48	Delet	77
49	Delet	77
50	Delet	77
51	Delet	77
52	Delet	77
53	Delet	77
54	Delet	77
55	Delet	77
56	Delet	77
57	Delet	77
58	Delet	77
59	Delet	77
60	Delet	77
61	Delet	77
62	Delet	77
63	Delet	77
64	Delet	77
65	Delet	77
66	Delet	77
67	Delet	77
68	Delet	77
69	Delet	77
70	Delet	77
71	Delet	77
72	Delet	77
73	Delet	77
74	Delet	77
75	Delet	77
76	Delet	77
77	Delet	77
78	Delet	77
79	Delet	77
80	Delet	77
81	Delet	77
82	Delet	77
83	Delet	77
84	Delet	77
85	Delet	77
86	Delet	77
87	Delet	77
88	Delet	77
89	Delet	77
90	Delet	77
91	Delet	77
92	Delet	77
93	Delet	77
94	Delet	77
95	Delet	77
96	Delet	77
97	Delet	77
98	Delet	77
99	Delet	77
100	Delet	77

