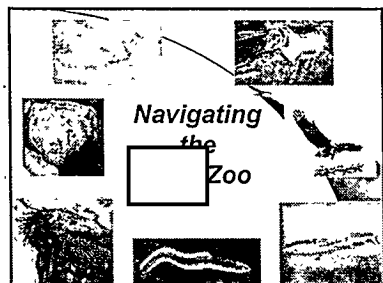


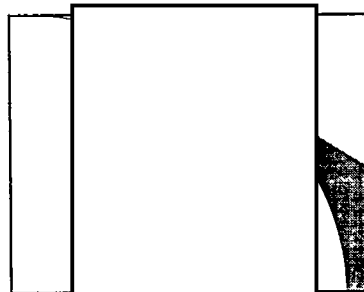
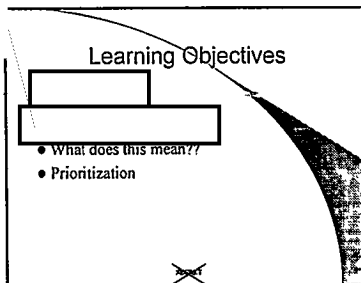
DATE: 02-07-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-07-2037

~~SECRET~~

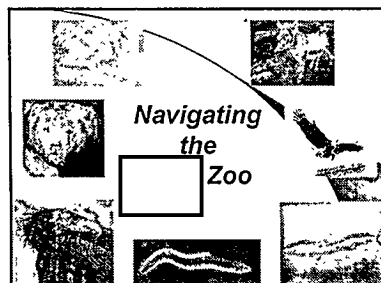
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



(S)



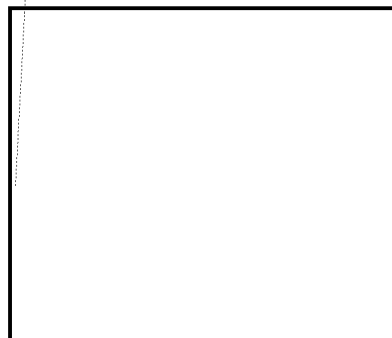
b1
b7E



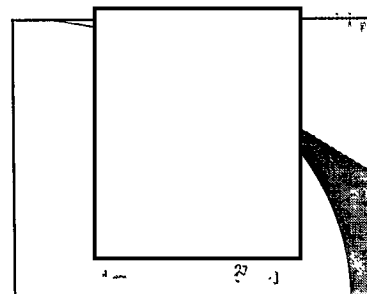
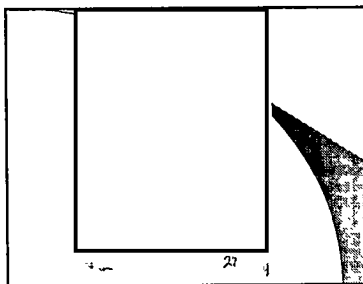
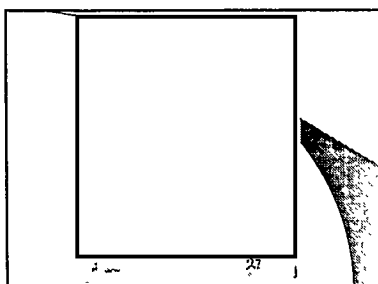
(S)



(S)



b1
b7E



b7E

~~SECRET~~

ACLURM042900

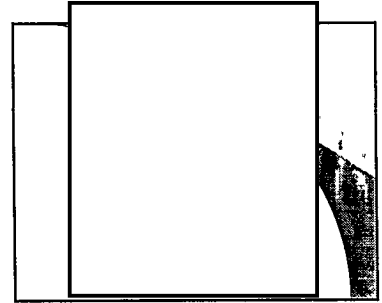
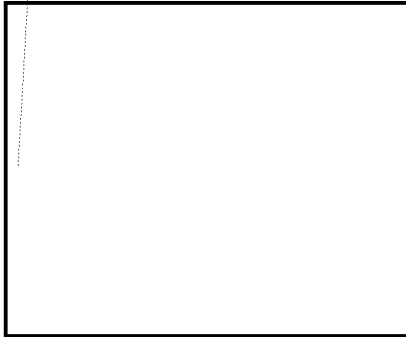
~~SECRET~~

b1
b7E

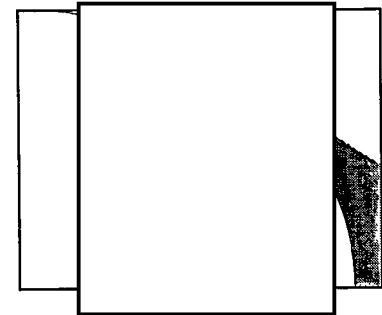
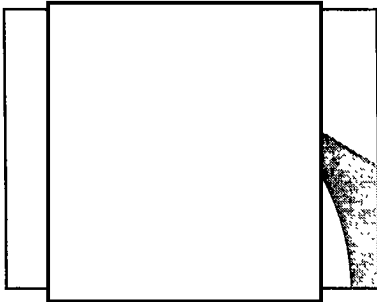
(S)



(S)

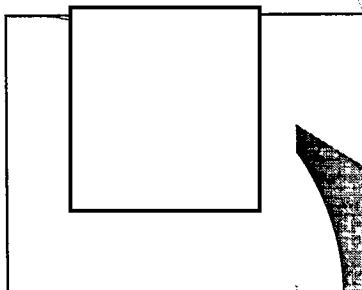
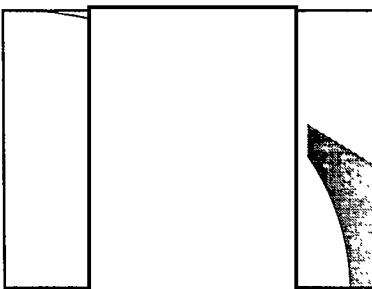


(S)



b1
b7E

(S)



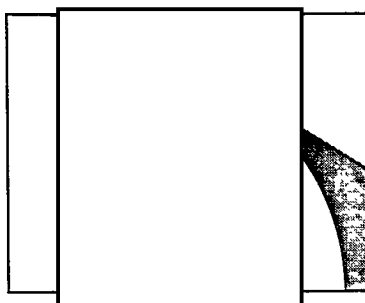
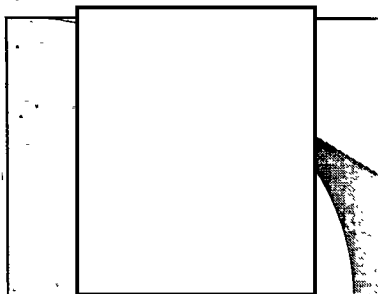
b1
b7E

~~SECRET~~

~~SECRET~~

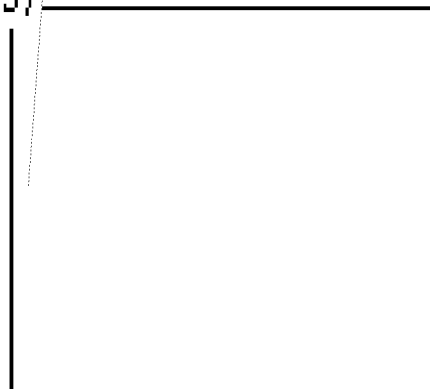
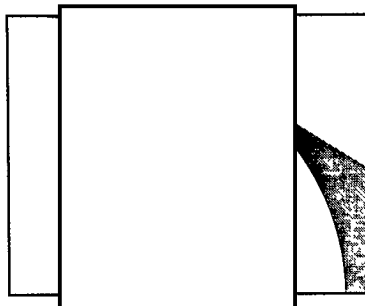
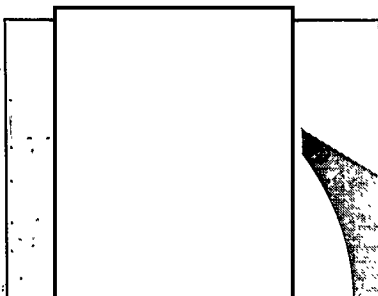
b1
b7E

(S)



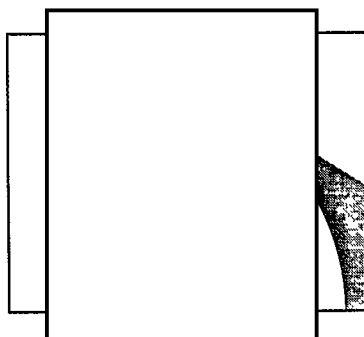
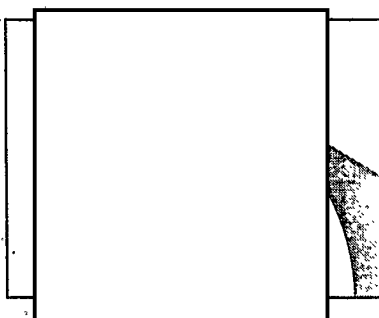
b1
b7E

(S)

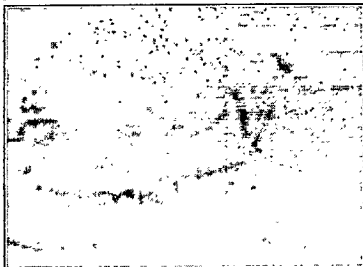


b1
b7E

(S)



~~SECRET~~



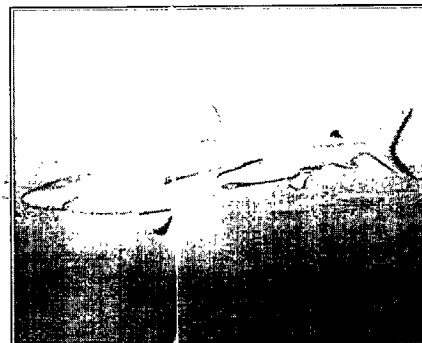
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 02-07-2012 BY 65179 DMH/STW



Navigating the Zoo



b7E



~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 01-27-2012

Counterintelligence Training Center
Counterintelligence Division



What You Need to Know
About Protecting Classified Information

This presentation is
unclassified

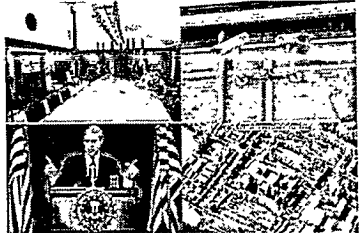
Counterintelligence Training Center Counterintelligence Division

Counterintelligence Training Center Counterintelligence Division

**FBI Failed to Classify Reports
Before Moussouni Had Them**

Counterintelligence Training Center Counterintelligence Division

Types of FBI Information



Counterintelligence Training Center Counterintelligence Division

b4

Executive Order 12958
Signed by President
Clinton effective
October 14, 1995



William Clinton

**Amended by
Pres. Bush
3/25/03**



Counterintelligence Training Center Counterintelligence Division

**Classified National
Security Information**



Information, which if disclosed, would
cause harm to the national security or
foreign relations of the U. S.

Counterintelligence Training Center Counterintelligence Division

Original Classification

The *INITIAL* determination which
establishes the precedent that the
information requires classification
and protection



Counterintelligence Training Center Counterintelligence Division

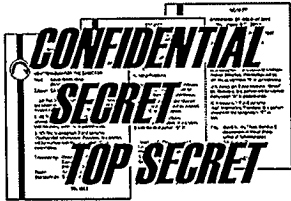
Classification Criteria

- A. Military plans, weapons or operations
- B. Foreign government information
- C. Intelligence activities, sources or methods
- D. Foreign affairs of the United States
- E. Scientific, technological or economic
- F. Nuclear materials or facilities
- G. Vulnerabilities or capabilities of systems
- H. Weapons of mass destruction

EO 12958 Section 1.4(c)

Counterintelligence Training Center Counterintelligence Division

Classification Levels

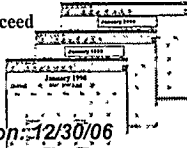


Counterintelligence Training Center Counterintelligence Division

Declassification Policy

OCA must set a date for
declassification of the information.

Must not exceed
25 years.



Declassify on: 12/30/06

Counterintelligence Training Center Counterintelligence Division

~~SECRET~~

ACLURM042904

FBI041804

Exemptions

The identity of a confidential human source or a human intelligence source is not subject to automatic declassification.

X1-X8 exemptions can no longer be used.



Declassify on: 25X1-human

Counterintelligence Training Center Counterintelligence Division

Classification Guides

Classification decisions made by OCA(s) which are published as classification policy for agency or community use.

Foreign Counterintelligence Investigations Guide (G-3)

Counterintelligence Training Center Counterintelligence Division

Derivative Method

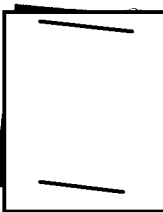
Incorporating, restating or generating in new form information that already has been classified....



Counterintelligence Training Center Counterintelligence Division

b7E

Marking Classified Documents

Counterintelligence Training Center Counterintelligence Division

b7E

(U) Portion Marking

(S) Indicate classification level of each portion of a document:

(C) Subject

(U) Paragraphs

(U) Graphics



(*) This is a chart

Counterintelligence Training Center Counterintelligence Division

b6
b7C

Portion Marking

Guid

(U) Indicate classification level of each portion of a document:

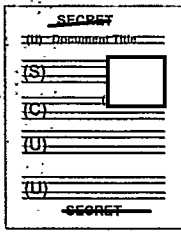
1 = Top Secret Friday
2 = Top Secret Friday 2006
3 = (S) Spies with the World Series

Counterintelligence Training Center Counterintelligence Division

b7E

b7E

Document Marking



Counterintelligence Training Center Counterintelligence Division

Page Marking

S	CO	UNCLASSIFIED
(U)	(U)	(U)
(S)	(C)	(U)
(C)	(C)	(U)
(U)	(U)	(U)
(U)	(U)	(U)
(U)	(U)	(U)
	CC	UNCLASSIFIED

Counterintelligence Training Center Counterintelligence Division

Original Classification

"Classified by" line
"Classified why" line
"Declassify on" line

Classified by : 7970
Reason: 1.4(c)
Declassify On: 1-25-07



Counterintelligence Training Center Counterintelligence Division

Derivative Classification

"Derived from" line _____
 "Declassify on" line _____

Derived from: source document
 Declassify On: 1-25-07

SECRET

Counterintelligence Training Center Counterintelligence Division

Derivative Classification

Derived from : FBI EC dated 1/21/04, captioned "Security Policy"
 Declassify On: 1/21/29

Derived from : Multiple Sources
 Declassify On: 1/21/29

Derived from : FBI EC captioned "Marking Policy"
 Declassify On: Source Marked X1, Date of source: 2/25/95

Counterintelligence Training Center Counterintelligence Division

Declassification and the G-3 Guide

Derived from : G-3
 Declassify On: (25 years from today)

FBI Security Memorandum
 Classified National Security Information
 3/31/04

Counterintelligence Training Center Counterintelligence Division

b7E

Community Marking

SECRET #20291009
 (U) Document Title _____
 (S) _____
 (C) _____
 (U) _____
 (U) _____
SECRET #20291009

Counterintelligence Training Center Counterintelligence Division

Transmittal of Classified Material

Counterintelligence Training Center Counterintelligence Division

Cover Sheets

CONFIDENTIAL
SECRET
TOP SECRET

Counterintelligence Training Center Counterintelligence Division

b7E

Within the Office

Counterintelligence Training Center Counterintelligence Division

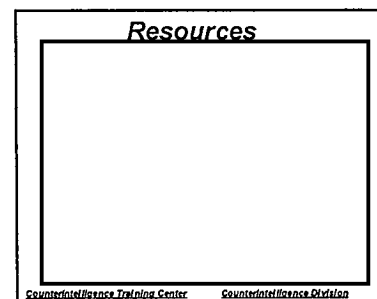
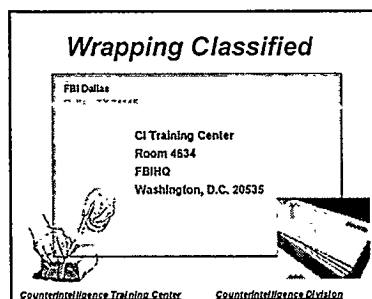
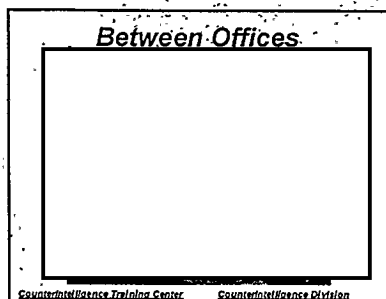
Within the Office

Counterintelligence Training Center Counterintelligence Division

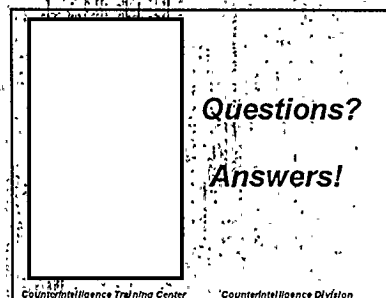
Between Offices

Counterintelligence Training Center Counterintelligence Division

b7E



b7E

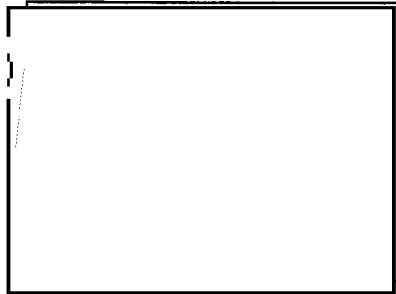


b7E

~~SECRET~~

(S)

(S)



Goals
• Make you aware these types of cases exist. • Familiarize you with a real-life example of how several different investigative techniques contributed to a successful investigation, and the pros and cons of these tools. • Warn you of potential pitfalls during such an investigation. • Show you that you can do this.

<u>FCI Investigations</u>
When you have eliminated the impossible, whatever remains, however improbable, must be the truth.

b1
b7E

200Q Techniques
• Electronic surveillance • Physical surveillance • Arrests • Interrogations • Search warrants • Trash cover • Forfeiture • Convictions – Federal Prison time

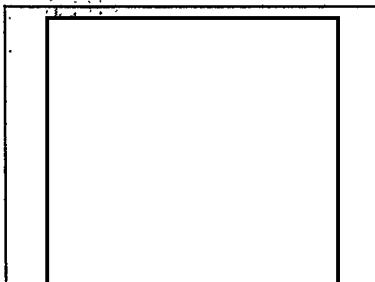
<u>Featuring...</u>
• FBI (FCI squad, [redacted] SSG, IAs, TTAs, ERT, FA, CART, SWAT, other divisions) • Other

Definitions

b1
b7E

(S)

(S)

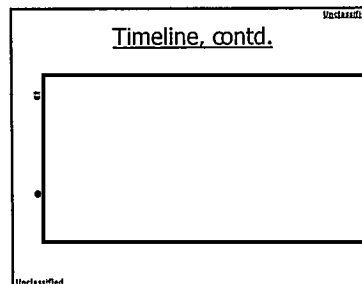
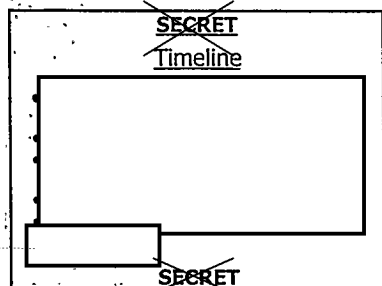


b1
b7E

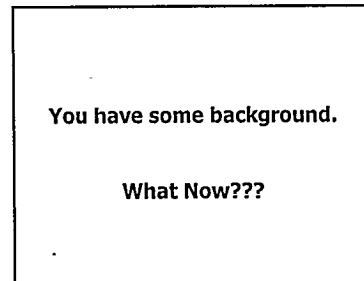
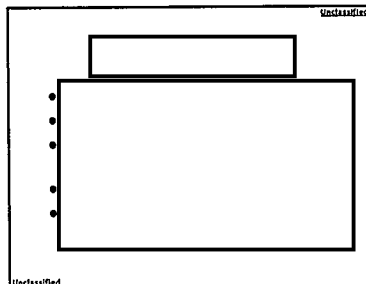
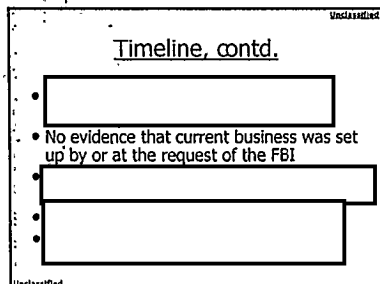
~~SECRET~~

~~SECRET~~

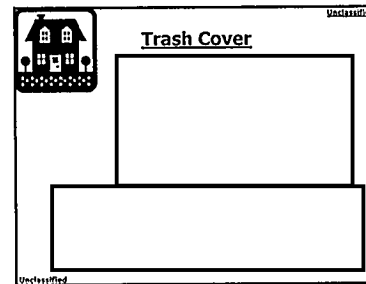
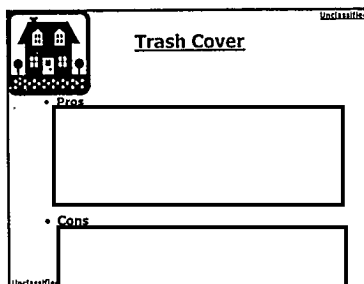
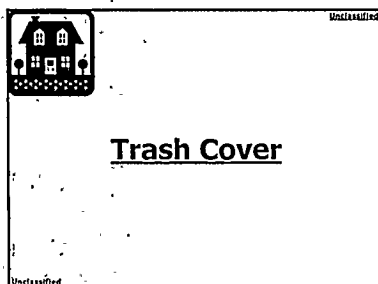
(S)



b1
b6
b7C
b7E



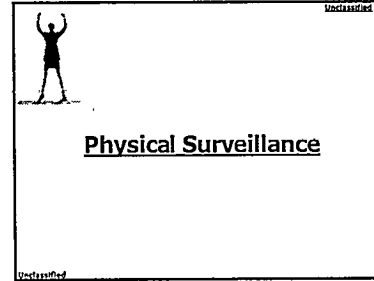
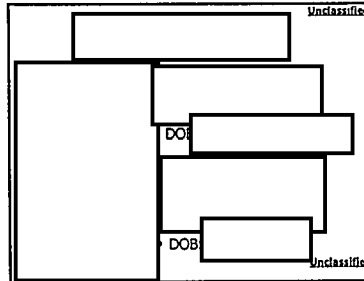
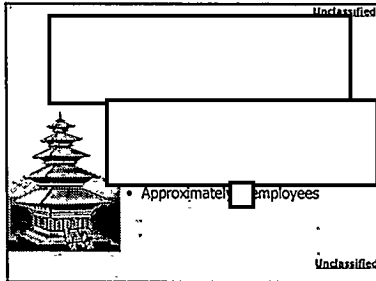
b6
b7C
b7E



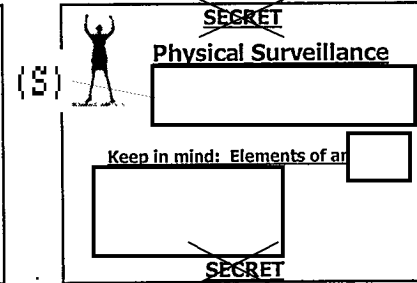
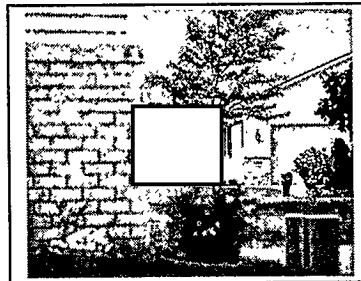
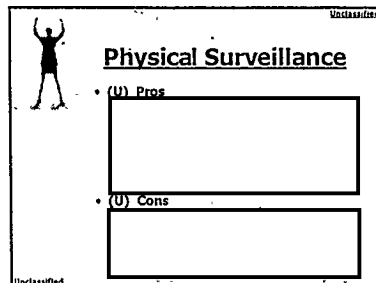
b7E

~~SECRET~~

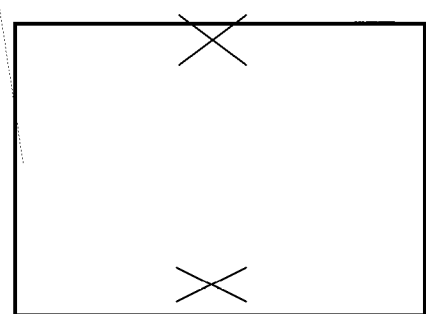
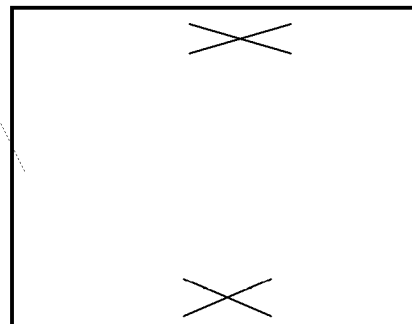
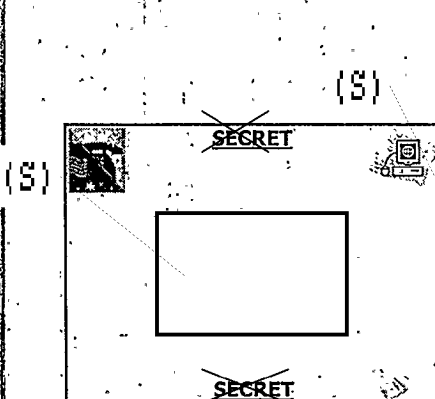
~~SECRET~~



b6
b7C
b7E

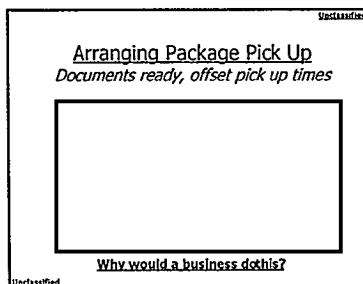
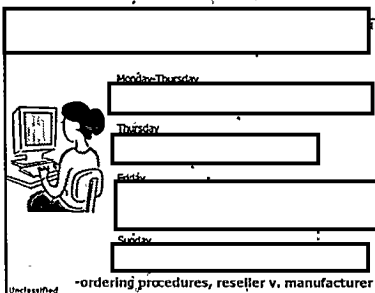


b1
b6
b7C
b7E

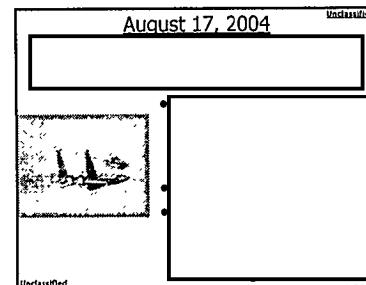
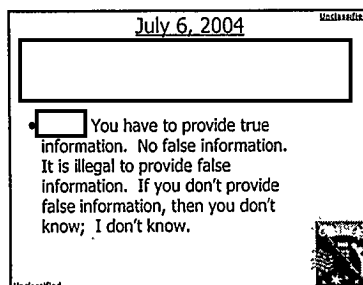
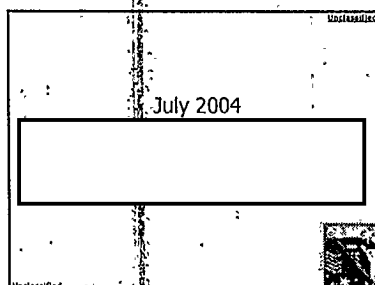


~~SECRET~~

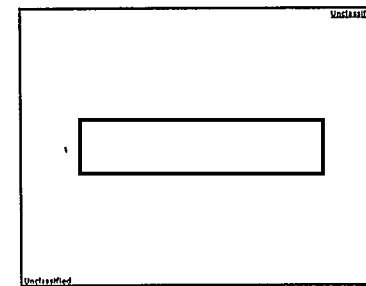
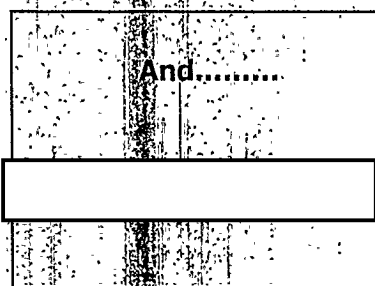
~~SECRET~~



b6
b7C
b7E



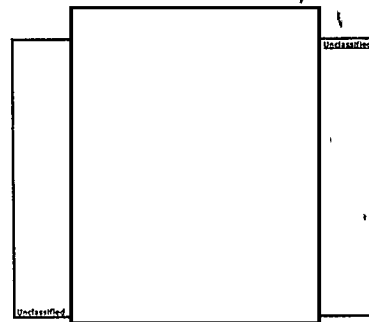
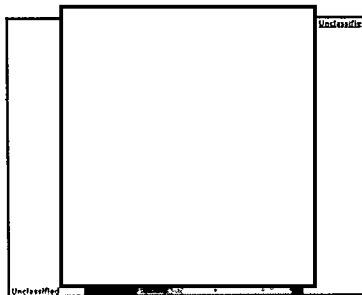
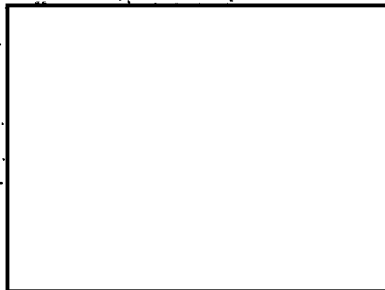
b6
b7C
b7E



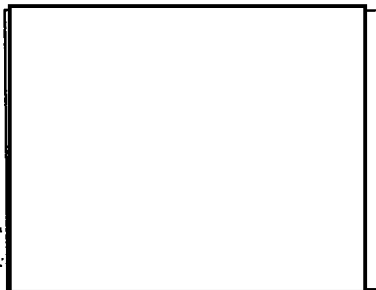
b7E

~~SECRET~~

~~SECRET~~



b7E



Working with Language Support

- Start early
- Evaluate the product early and throughout
- Engage and train
- Provide feedback (+praise)
- Defend + motivate
- Emotional issues (interrogations)
- Tactical issues

Working with Language Support (continued)

- Interviews
 - Preparation (names, terms, facts)
 - Cultural advice
 - Positioning
 - Take breaks
- Trial preparation
 - Certified translations
 - Testimony prep (include cross)

If you want to make an arrest...

- Declassify information needed for prosecution
- AG authority
- Licensing determinations

~~SECRET~~

excellent
(and last) North American
Adventure



September 30, 2004

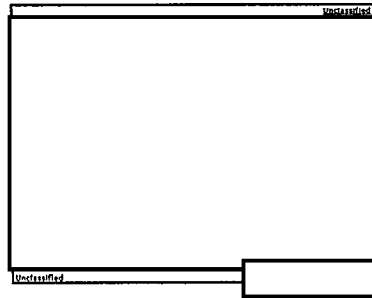
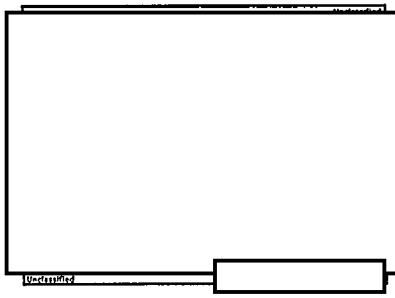
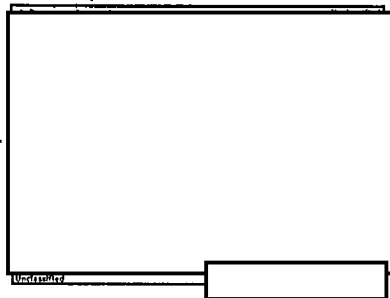


- Arrest warrants for
- Search warrants for office/residence, safe deposit boxes.
- Subsequent search warrant for computer, luggage.
- Four interviews/interrogations. All waived rights and agreed to answer questions.

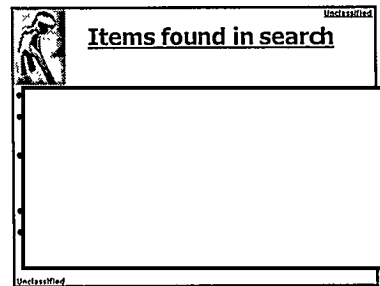
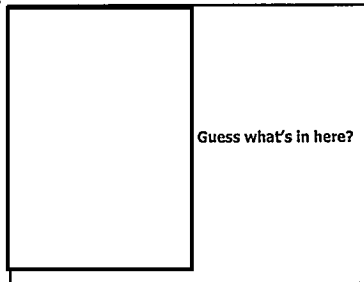
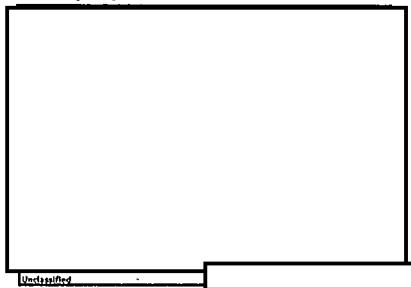
b1
b6
b7C
b7E

~~SECRET~~

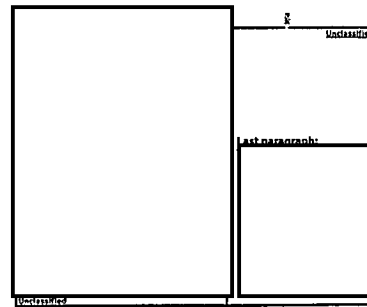
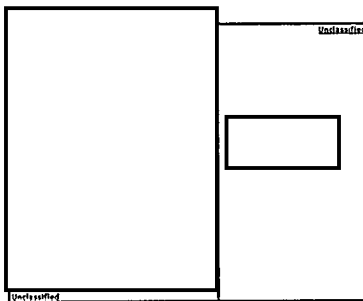
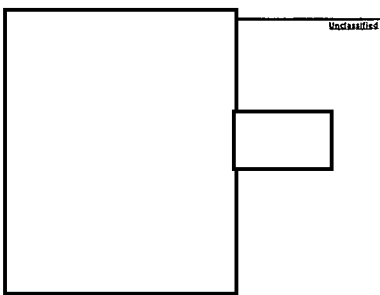
~~SECRET~~



b7E



b7E



b7E

~~SECRET~~

~~SECRET~~

Resignation Letter

Unclassified

Continuity Letter

Unclassified

fax from [redacted]

Unclassified

b6
b7C
b7E

Search document excerpts [redacted]

Unclassified

Search document excerpts [redacted]

Unclassified

One big (previously) happy conspiracy

Unclassified

b6
b7C
b7E

(S)

(S)

~~SECRET~~

(U)

(U) Several others

~~SECRET~~

X

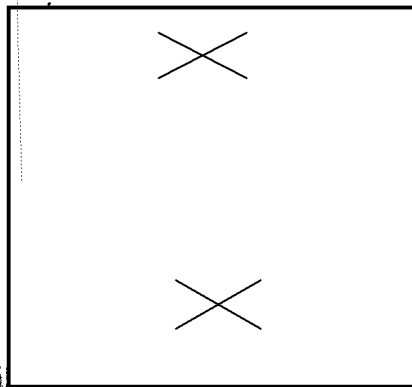
X

b1
b7E

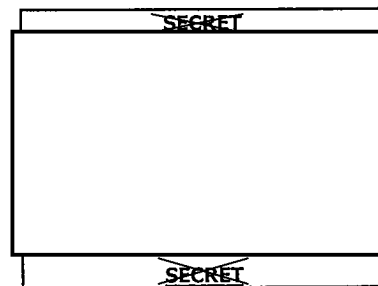
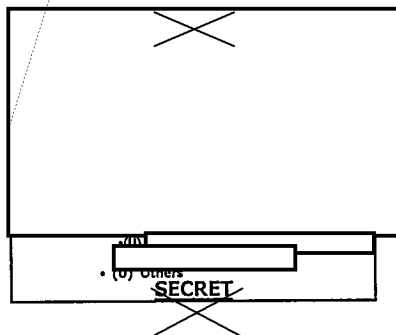
~~SECRET~~

~~SECRET~~

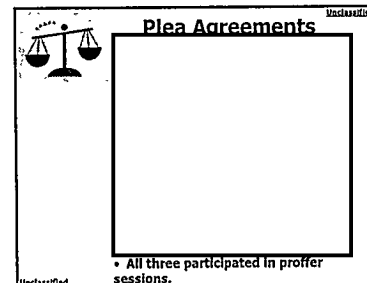
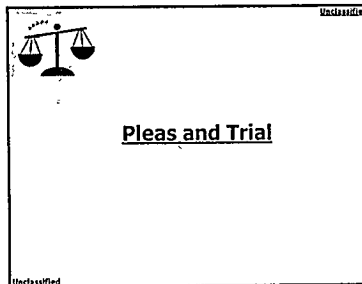
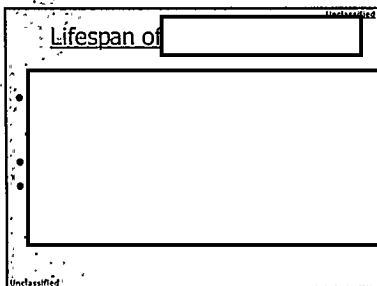
(S)



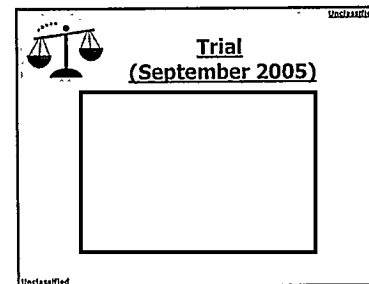
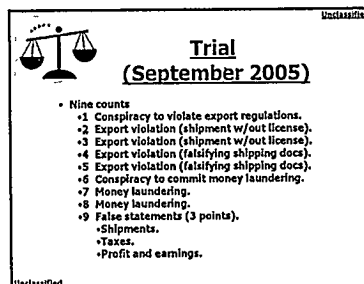
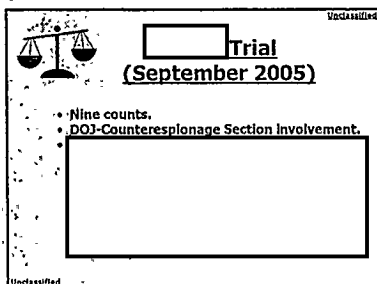
(S)



b1
b7E



b6
b7C
b7E



b6
b7C
b7E

~~SECRET~~

~~SECRET~~

 **Trial**
(September 2005)

- **SA testimony**
 - Seizing Agent, Trash Cover Agent, read tech cuts into record
- Handling Agent
 - Assessment
 - Recording
 - Case Agent - Cross Examination

[Redacted]

 **Trial**
(September 2005)

- **Defense argument themes**
 - I didn't know.
 - I don't remember.
 - I didn't understand English on 09/30/2004.
 - My wife did it all, without my knowledge.
 - We did talk about the business, but it was only 2-3% of the time.
 - I never noticed that we made \$100,000 a year more than we reported on taxes.

 **Trial**
(September 2005)

- Key moment (during cross examination of [Redacted])
 - AUSA Q: "When you are talking to the FBI, you know it's important to tell the truth, right?"
 - [Redacted] answer: [Redacted]
 - 2 1/2 hours of deliberation (over lunch).
 - **Verdict: Guilty on all 9 counts.**

b6
b7C
b7E

 **Sentencing**

[Redacted]

- Defense argued for consideration [Redacted] contributions to his US employment to the FBI in his [Redacted] Also included character testimonials. Also argued, unsuccessfully, that parts were [Redacted] was most responsible.

 **Forfeiture + Fines**

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

FISA v. Title III

[Redacted] appealed to Seventh Court of Appeals on grounds that evidence gathered under FISA cannot be used in domestic criminal prosecution (ie Title III should have).

- From the ruling, "Probable cause to believe that a foreign agent is communicating with his controllers outside our borders makes an interception reasonable. If, while conducting this surveillance, agents discover evidence of a domestic crime, they may use it to prosecute for that offense. That the agents may have known they were likely to hear evidence of domestic crime does not make the interception less reasonable than if they were ignorant of the possibility."

b6
b7C
b7E

(S)

[Redacted]

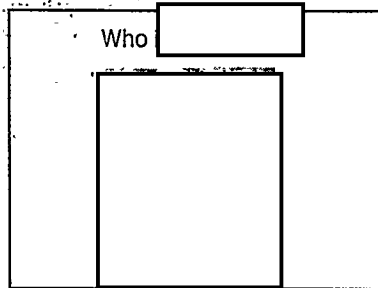
[Redacted]

[Redacted]

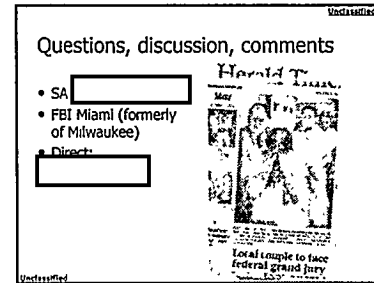
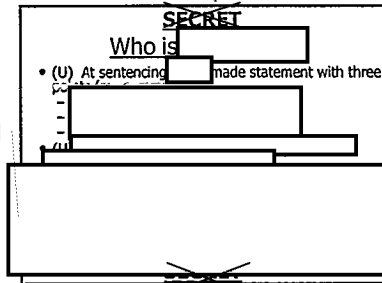
b1
b7E

~~SECRET~~

~~SECRET~~

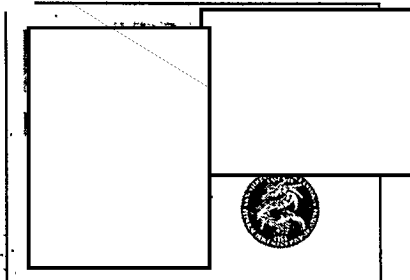


(S)



b6
b7C
b7E

(S)



b1
b7E

~~SECRET~~

FCI Investigations

When you have eliminated the impossible, whatever remains, however improbable, must be the truth.

FISA vs. Prosecution

FCI vs. Criminal

IIRs vs. Arrests, Indictments, Convictions

Working with Language Support

- Start early
- Evaluate the product early and throughout
- Engage and train
- Provide feedback (+praise)
- Defend + motivate
- Emotional issues (Interrogations)
- Tactical Issues

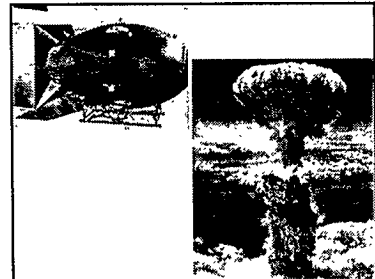
Working with Language Support (continued)

- Interviews
 - Preparation (names, terms, facts)
 - Cultural advice
 - Positioning
 - Take breaks
- Trial preparation
 - Certified translations
 - Testimony prep (include cross)

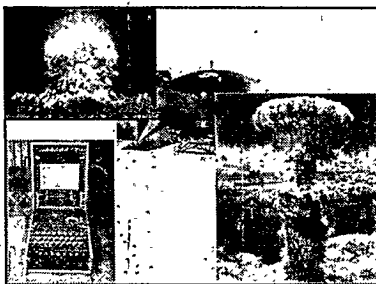
Proving Willful Conduct

- 1)
- 2)
- 3)

*****Doing something economically inefficient.*****



b7E



DATE: 02-07-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-07-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

A Continuing Multi-Agency/
Multi-Jurisdictional
Investigation

- March to October 2004
- MW Case Agent

b6
b7C
b7E

History

History

History

b6
b7C
b7E

Key event...

Timeline...

(S)

Timeline, cont..

April 2004 to October 2004 -

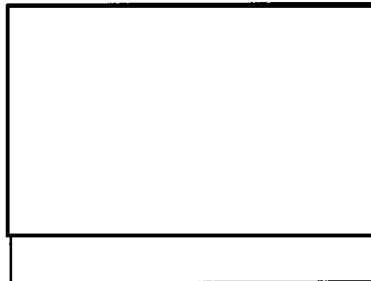
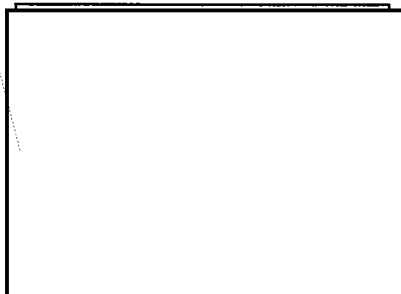
b1
b7E

~~SECRET~~

ACLURM042920

~~SECRET~~

(S)

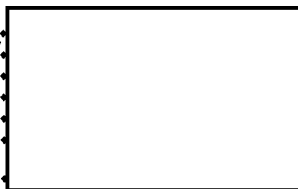


September 30, 2004 Arrest and
Search results



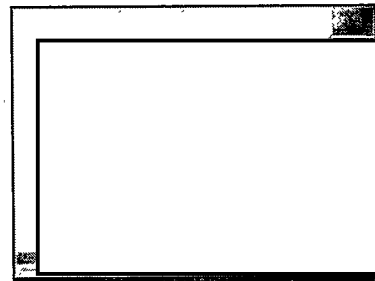
b1
b6
b7C
b7E

Identified End-Users...

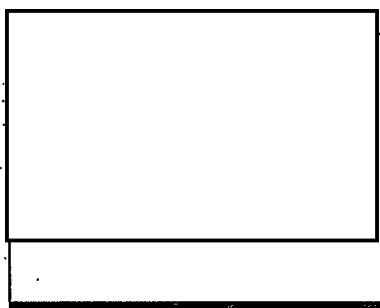


(S)

Results of



b1
b6
b7C
b7E



(S)

Gains...



(S)

The Investigation Continues...

♦ March, 2005 - SL begins electronic
surveillance (email) of [redacted]

♦ "XXXXXXXXXX@hotmail.com"

b6
b7C
b7E

b1
b7E

~~SECRET~~

~~SECRET~~

Investigation continues...
[redacted]
identified as representing [redacted]
[redacted]
[redacted]...proves unsuccessful.

Investigation continues...
[redacted] ceases 'cooperation'
eventually pleads guilty, April, 2006.

Investigation continues...
Following deportation to [redacted]
[redacted]
[redacted] using the
same email address...
"XXXXXXXXXX@hotmail.com"

b6
b7C
b7E

(S)

[redacted]

(S)

[redacted]

(S)

[redacted]

b1
b7E

(S)

[redacted]

[redacted]
[redacted] using
XXXXXXXXXX@hotmail.com to conduct
business with [redacted] (SD)
[redacted] is helping [redacted] establish a
[redacted]

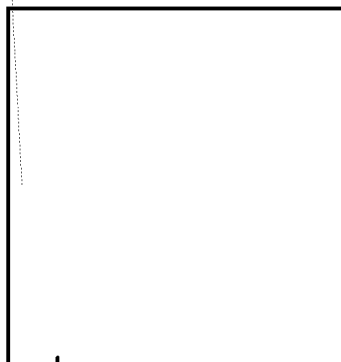
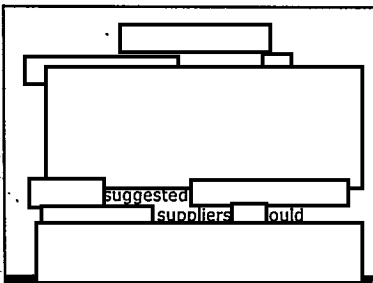
[redacted]

b6
b7C
b7E

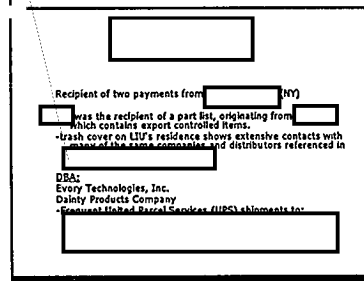
~~SECRET~~

~~SECRET~~

(S)

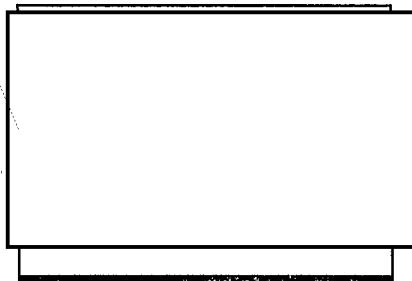


(S)

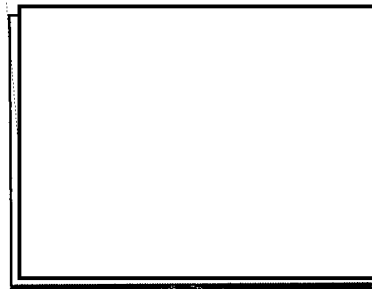
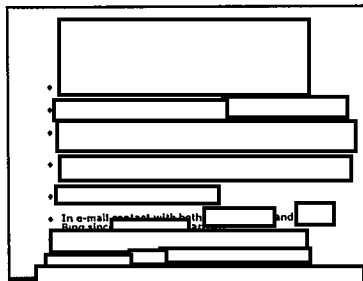


b1
b6
b7C
b7E

(S)

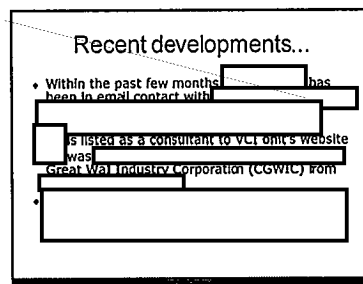
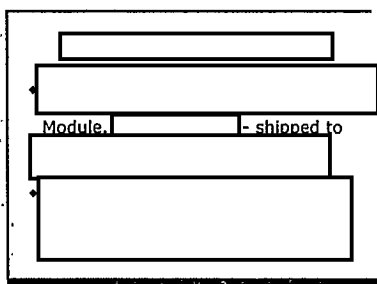


(S)



b1
b6
b7C
b7E

(S)



(S)



b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

b6
b7C
b7E

Just last week...

[Redacted]

[Redacted]

[Redacted]

Merry Christmas..

[Redacted]

Known Violations

- Violation of Export Laws (CCL)
- Extensive use of email / telephone to facilitate transactions...
- Extensive use of the mail / shipping companies...
- Continuing falsification of Shipper's Export Declarations...
- Money Laundering...
- Tax Evasion...

[Redacted] address:

Very similar to:

Which is used by:

[Redacted]

Some issues..

- Dissemination of [Redacted] material...LHM...AG use authority [Redacted] not yet...
- Need for [Redacted] determinations...
- Availability of [Redacted]

Strengths...

- Single POC at FBI/[Redacted] HQ for entire multi-jurisdictional investigation to facilitate information flow to all involved investigators...and quickly address issues..
- Follow-up leads sent to new Field Offices to ensure investigations are pursued in a timely, coordinated manner...
- Single OIPR attorney to facilitate all [Redacted] proceedings...

b1
b7E

(S)

The way ahead..

- [Redacted]
- Continue to identify IIS players
 - Maximum [Redacted]
 - RICO?

Questions or Comments

Supervisory Special Agent

[Redacted]
FBI Headquarters

b6
b7C
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b7E

[Redacted]

Weapons of Mass Destruction Directorate

SI [Redacted]
This presentation is classified "Secret/NoFORN"

WMD Directorate

[Redacted]

[Redacted] Mission

[Redacted]
of weapons of mass destruction (WMD)-

[Redacted]

- WMD can be chemical, biological, radiological, or nuclear in nature.

b6
b7C
b7E

CPOU's Role

The CPOU maintains [Redacted]

[Redacted]

This responsibility is carried out in close [Redacted]

[Redacted]

CPOU Functions and Working Relationships

- [Redacted] WMD counterproliferation investigations, i.e., those with a CPOU designation.
- Represents the WMDD on all [Redacted] matters.
- Maintains a comprehensive knowledge of nation-state WMD [Redacted] to CP [Redacted]
- [Redacted]
- [Redacted] is the local point in the WMDD for all [Redacted]

FBI [Redacted]

[Redacted]

Joint Activities [Redacted]

- [Redacted] have law enforcement responsibility for the export of restricted WMD and dual-use items.
- FBI and [Redacted]
- FBI has primary jurisdiction regarding export violations where there is a [Redacted]

b1
b6
b7C
b7E

CPOU Counterproliferation Programs

- Chemical Weapons Convention (CWC) interagency participation
- Proliferation Security Initiative (PSI) interagency participation

Chemical Weapons

[Redacted]

Federal Bureau of Investigation

- Chemical Weapons Convention Implementation Act Public Law 105-277
- Mandates FBI Presence at Each U.S. Commercial Inspection

[Redacted]

- Dec 2002 - US National Strategy to Combat WMD called for enhanced [Redacted]
- Announced by President Bush in Krakow, Poland on May 31, 2003
- PSI Statement of Interdiction Principles - is a political commitment to act against proliferation-related shipments to or from states or non-state actors of concern

b7E

~~SECRET~~

AQURM042925

FBI041825

~~SECRET~~

(5)

~~1 Special/Not on~~

~~Secret/NoForN~~

b1
b7E

- CP is a top priority for the U.S.
- Often, U.S. firms are unwitting participants in proliferation networks due to the fraudulent use of front companies or overseas intermediaries to conceal the identities of the actual end users
- Some proliferant countries are relying on *witting* U.S.-based companies and/or procurement agents
- Cases indicate a growing need to more aggressively address the exploitation of U.S. technology

~~Secret/No For~~

(S)

- See V/Notes

- CPOU, along with other Analysts in the WMDD, Counterintelligence Division, and other Divisions, regularly disseminate information to the U.S. Intelligence Community.
- Other types of Reports are regularly generated including strategic and tactical analysis to support FBI Field Office investigations and other customers.

- CPOU receives intelligence from the USIC which

Samples of the reports and assistance we provide

- b1
b7E

151

151

151

121

121

Questions?

b1
b6
b7C
b7E

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Weapons of Mass Destruction Directorate

Counterproliferation Operations Unit

SM [redacted]
August 13, 2007
The protection is against [redacted]

WMD Directorate

CP Definition

- Counterproliferation is the [redacted]
[redacted]
of weapons of mass destruction (WMD)-
[redacted]
- WMD can be chemical, biological,
radiological, or nuclear in nature.

b7E

CPOU's Role

The CPOU maintains [redacted]
[redacted]
[redacted]
This responsibility is carried out in close
[redacted]

Activities in the U.S.

- CP is a top priority for the USIC.
- Often, U.S. firms are unwitting participants in proliferation networks due to the fraudulent use of front companies or overseas intermediaries to conceal the identities of the actual end users.
- Some proliferant countries are relying on willing U.S.-based companies and/or procurement agents.
- Main countries of concern: [redacted]
- Cases indicate a growing need to more aggressively address the exploitation of U.S. technology.

CPOU Functions and Working Relationships

- Has programmatic oversight for WMD counterproliferation investigations, i.e., those with the "Q" designation.
- Represents the WMDD on all CP investigative and operational matters.
- Maintains a comprehensive knowledge of nation-state WMD programs.
- Provides strategic, operational and tactical analytic support to CP operations and investigations.
- Establishes, maintains, and facilitates USIC CP liaisons.
- [redacted]
- CPOU serves as the focal point in the WMDD for all [redacted] and [redacted]

b7E

Joint Activities [redacted]
[redacted] have law enforcement
responsibility for the export of restricted WMD
and dual [redacted]
FBI and [redacted]

FBI has primary jurisdiction regarding export
violations where there is a [redacted]
[redacted]

CPOU Counterproliferation Programs

- Chemical Weapons Convention (CWC) interagency participation
- Proliferation Security Initiative (PSI) interagency participation

Chemical Weapons

Federal Bureau of Investigation

- Chemical Weapons Convention
Implementation Act Public Law 105-277
Mandates FBI Presence at Each U.S.
Commercial Inspection

b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

- Dec 2002: US National Strategy to Combat WMD called for enhanced [redacted]
- Announced by President Bush in Krakow, Poland on May 31, 2003
- PSI Statement of Interdiction Principles - is a political commitment to act against proliferation-related shipments to or from states or non-state actors of concern

(5)

- Representatives from FBI [redacted] Treasury, and [redacted] working together to take appropriate action.

Interagency Programs, Assignments, and Meetings

b7E

~~Secret~~
Analytical Resources and Tools
Used by CPOU

- Other USIC traffic and reports
- Internet

Intelligence Dissemination

- CPOU, along with other Analysts in the WMDD, Counterintelligence Division, and other Divisions, regularly disseminate information to the U.S. Intelligence Community.
- Other types of Reports are regularly generated including strategic and tactical analysis to support FBI Field Office investigations and other customers.
- CPOU receives intelligence from the USIC which

CPOU Assistance and Production

Samples of the reports and assistance we provide

- Case generation ECs and teletypes
- [REDACTED] Questions
- Tactical case support
- CP Briefings/Presentations
- On-Site Field support

b1
b7E

(S)

(5)

(S)

(S)

(S)

115

[illegible]

**Counterproliferation Operations
Unit**

Questions?

b7E

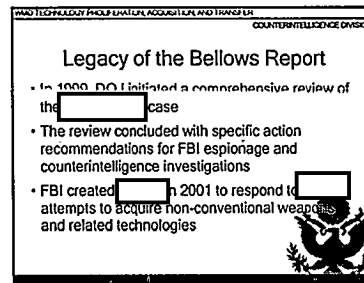
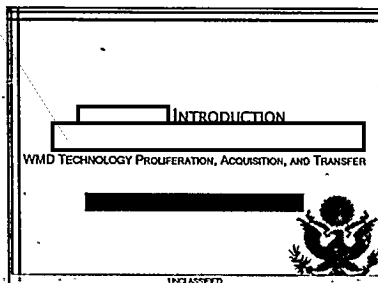
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

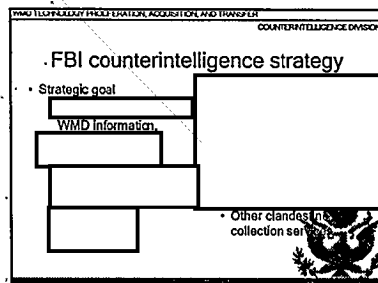
~~SECRET~~

(S)



b1
b6
b7C
b7E

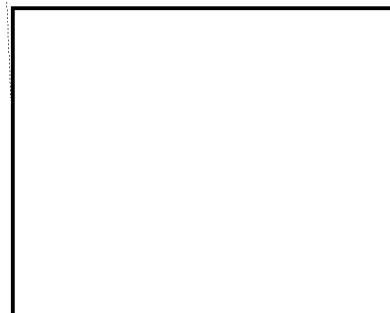
(S)



(S)

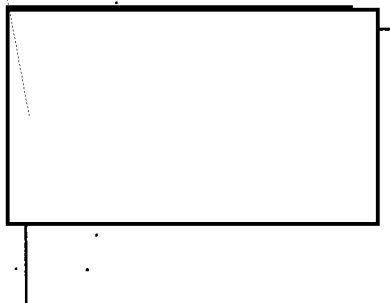


(S)

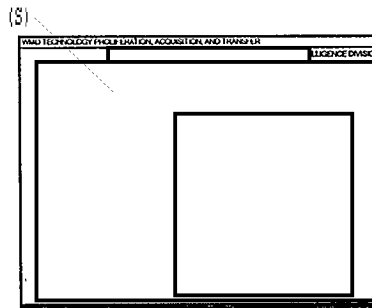


b1
b7E

(S)



(S)

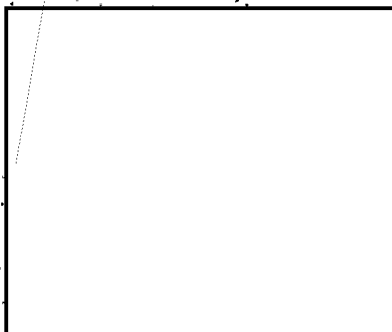


b1
b7E

~~SECRET~~

~~SECRET~~

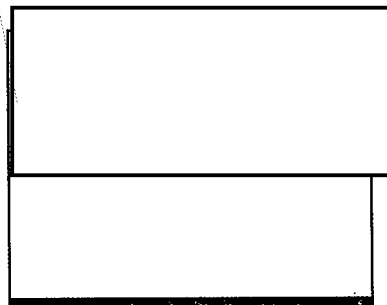
(S)



(S)



(S)



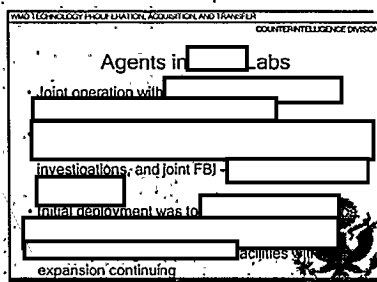
b1
b7E

(S)



b1
b7E

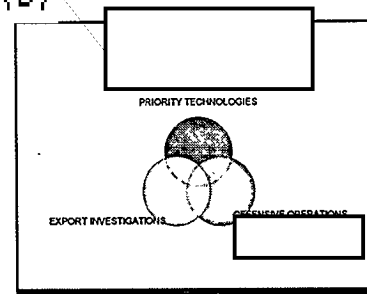
(S)



(S)



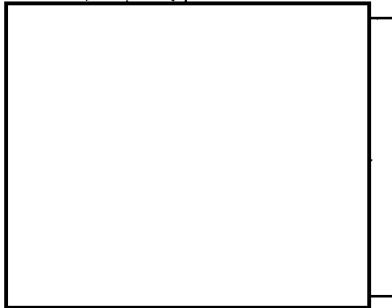
(S)



b1
b7E

~~SECRET~~

~~SECRET~~



(S)

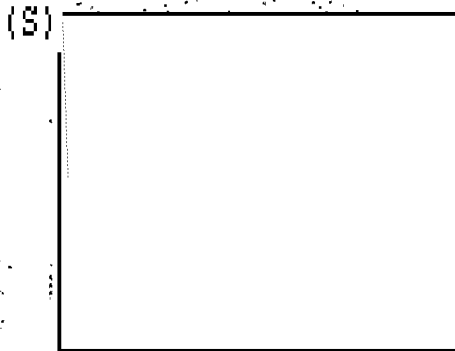
(S)

(S)

- Identify and initiate new investigations / operations
- Establish 'Monthly' CB Working Group at FBIHQ
- Response programs provide
- Cases worked to maximize Counterintelligence / Possible Intelligence

Why us and why now?

b1
b7E



WMD TECHNOLOGY PROLIFERATION, ACQUISITION, AND TRANSFER (WMD-TACT) DIVISION

Operational techniques

- Physical surveillance
- Mail and trash covers
- NSLs
- Grand Jury Subpoenas

WMD TECHNOLOGY PROLIFERATION, ACQUISITION, AND TRANSFER (WMD-TACT) DIVISION

Records and liaison

- Government records

b1
b7E

WMD TECHNOLOGY PROLIFERATION, ACQUISITION, AND TRANSFER (WMD-TACT) DIVISION

Other sources

- Commercial sources
- Analytic tools
- Dunn & Bradstreet

WMD TECHNOLOGY PROLIFERATION, ACQUISITION, AND TRANSFER (WMD-TACT) DIVISION

Frequent partners

WMD TECHNOLOGY PROLIFERATION, ACQUISITION, AND TRANSFER (WMD-TACT) DIVISION

Online resources

- Program descriptions and points-of-contact on
- Library of government and think tank publications on WMD proliferation, export control, language tools, and technology transfer
- Competent and efficient SSA and intelligence analyst support for field squads and intelligence groups

b1
b7E

~~SECRET~~

~~SECRET~~

Comments or questions?

SSA



UNCLASSIFIED

b6
b7C

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

 PRESENTATION FOR
GIOPs Course

[Redacted]

FOR OFFICIAL USE ONLY
UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The Threat to U.S. National Security

- The U.S. has the most advanced economy in the world
- Agents of foreign powers and others are aggressively attempting to acquire sensitive U.S. military technologies and information to steal our edge

[Redacted]



UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The Threat to U.S. National Security

"The U.S. government has identified 21 countries - of which Iran, North Korea, and Cuba are the most concerning - with the capability to either develop WMD systems or acquire export-controlled WMD and dual-use items and sensitive technologies."

"...stealing and compromising of classified and non-classified technologies are occurring at levels previously unknown."

 Robert S. Mueller, III
January 11, 2007
Statement before the Senate Select Committee on Intelligence

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

Counterintelligence:

- Counterterrorism:
- Terrorist groups acquiring U.S. military technology to arm insurgents

Organized Crime:

[Redacted]

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Reasons for [Redacted]

- The U.S. currently prohibits to some degree, the export and sale of defense articles [Redacted] as ITAR Sec. 120.1

[Redacted]

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The FBI's Role

- Enforcement authority is relatively new
- On Nov. 5, 2004, the Attorney General signed an order granting the FBI concurrent criminal jurisdiction in export matters with a counterintelligence nexus.

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."

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

What the FBI Contributes

- Unique dual-mission integrating traditional law enforcement with intelligence collection
- Largest complement of agents, analysts, linguists, and surveillance specialists
- Provide valuable intelligence to the USIC
- Foreign Intelligence Surveillance Act (FISA)
- Certain exemptions to the ITAR in UCOs
- Neutralization and intelligence collection through criminal prosecution

[Redacted]

UNCLASS / FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Investigative Goals

- Identify [Redacted]
- Disrupt [Redacted]
- Observe the behavior of [Redacted]

[Redacted]

UNCLASS / FOLD

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Joint Effort

- Cooperation is the key to success
- 2001 USA Patriot Act brings down "the walls"

[Redacted]

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Liaison with Regulatory Agencies

To accomplish our goals we must have effective liaison with those agencies [Redacted]

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Who Controls What ?

Defense Articles	Dual-use Items
[Redacted]	[Redacted]

b7E

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

[Redacted]

[Redacted]

[Redacted]

UNCLASS # FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Defense Articles

- If an item was specifically [Redacted] is a defense article and [Redacted]

[Redacted]

UNCLASS # FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

[Redacted]

STAR § 120.10

AP Associated Press
Four charged in alleged conspiracy to smuggle U.S. military secrets
China

U.S. vs. [Redacted]

[Redacted]

UNCLASS # FOLD

b7E

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

[Redacted]

UNCLASS # FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

[Redacted]

[Redacted]

UNCLASS # FOLD

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Registration

- Any person who engages in the U.S. in the business of either manufacturing or exporting defense articles or furnishing defense services is required to register [Redacted]
- Brokers - "Any U.S. person, wherever located..."
- \$1750 annually
- Registration data is available - Names, DOB, POB, SSN, etc.

UNCLASS # FOLD

b7E

~~SECRET~~

~~SECRET~~

(S)

FEDERAL BUREAU OF INVESTIGATION WFO DIRECTORATE

License Determinations

[Redacted]

[Redacted]

b1
b7E

FEDERAL BUREAU OF INVESTIGATION WFO DIRECTORATE

UCO Support

- FBI UCOs that involve [Redacted]
- UIC companies can be red started [Redacted]
- [Redacted]
- [Redacted]
- No objection letters

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION WFO DIRECTORATE

Questions ?

[Redacted]

SSA [Redacted]

[Redacted] FBIHQ

b6
b7C
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE



PRESENTATION FOR THE
Counterintelligence Operations
and Investigations Course

[Redacted]

THIS BRIEFING IS UNCLASSIFIED
FOR OFFICIAL USE ONLY

UNCLASSIFIED

(S)

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The Threat to U.S. National Security

The U.S. government has identified 21 countries – of which Russia, North Korea, and China are of the greatest concern – with the capability to either develop WMD systems or acquire export-controlled WMD and dual-use items and sensitive technologies.

- Agents of foreign powers and others are aggressively attempting to acquire sensitive U.S. military technologies and information to steal our edge.

[Redacted]



UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The Threat to U.S. National Security

The U.S. government has identified 21 countries – of which Russia, North Korea, and China are of the greatest concern – with the capability to either develop WMD systems or acquire export-controlled WMD and dual-use items and sensitive technologies.

“...stealing and compromising of classified and non-classified technologies are occurring at levels previously unknown.”

 Robert S. Mueller, III
January 11, 2007
Statement before the Senate Select Committee on Intelligence

UNCLASSIFIED

b1
b6
b7C
b7E

(S)

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

- Counterintelligence:

(S)

- Counterterrorism:
– Terrorist groups acquiring U.S. mil. art. technology to arm insurgents

(S)

- Organized Crime:

[Redacted]

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Reasons for Illegal Acquisition

- Advance R&D efforts
- Maintain aging aircraft and other platforms
- Exploit U.S. vulnerabilities
- Reverse engineering

(S)

(S)

– The U.S. currently prohibits to some degree, the export and sale of defense articles to [Redacted] (ITAR Sec. 125.1)

UNCLASSIFIED

(S)

(S)

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

UNCLASSIFIED

b1
b7E

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

The FBI's Role

- On 11/05/2004, the Attorney General signed an order granting the FBI concurrent 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”.

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

Joint Effort

- Cooperation is the key to success
- 2001 USA Patriot Act brings down “the walls” which hindered information sharing
- Frequent partners:

[Redacted]

FEDERAL BUREAU OF INVESTIGATION WMD DIRECTORATE

What the FBI Contributes

- Unique dual-mission integrating traditional law enforcement with intelligence collection
- Largest complement of agents, analysts, linguists, and surveillance specialists
- Provide valuable intelligence to the USIC
- Foreign Intelligence Surveillance Act (FISA) tools
- Certain exemptions to the ITAR in UCOs
- Neutralization and intelligence collection through criminal prosecution



UNCLASSIFIED

b7E

~~SECRET~~

ACLURM042936

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

Investigative Goals

- Identify foreign agents and procurement activities
- Disrupt attempts to acquire sensitive technologies and information
- Change the behavior of

UNCLASSIFIED FOLD

(S)

(S)

(S)

(S)

b1

b7E

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

Who Controls What ?

Regulated Agent	
Investigative Agency	
Statute	
Implementing Regulations	
Control Unit	

UNCLASSIFIED FOLD

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

UNCLASSIFIED FOLD

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

Defense Articles

If an item was specifically

UNCLASSIFIED FOLD

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

UNCLASSIFIED FOLD

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

Registration

- Any person who engages in the U.S. in the business of either manufacturing or exporting defense articles or furnishing defense services is required to register
- Brokers - "Any U.S. person, wherever located..."
- \$1750 annually
- Registration data is available - Names, DOB, POB, SSN, etc.

UNCLASSIFIED FOLD

b7E

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

License Determinations

UNCLASSIFIED FOLD

(S)

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

UNCLASSIFIED FOLD

(S)

FEDERAL BUREAU OF INVESTIGATION WHO DIRECTORATE

UNCLASSIFIED FOLD

b1

b7E

~~SECRET~~

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION		WFO DIRECTORATE
	Support	
		
UNCLASSIFIED		

FEDERAL BUREAU OF INVESTIGATION		WFO DIRECTORATE
Questions ?		
		
SSA		
	(FBIHQ)	

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE

SSA [redacted]
SSA [redacted]
Counterintelligence [redacted]
AGC [redacted]
Office of the General Counsel
National Security Law Branch
August 2006



The mission of the

[redacted]

- To Administer, Coordinate and Support National Security Activities

Coordination with:

- Case Agent/ Field Division
- Field Undercover Coordinator
- National Security Law Branch

[redacted]

b6
b7C
b7E

[redacted]

[redacted] Function

[redacted]

- On-Site review of UCO(s)
- Liaison with Field UC Coordinators

WHAT IS AN UNDERCOVER OPERATION?

[redacted]

b7E

National Security Operations

- The May 2002 AG Criminal Guidelines are generally not applicable
- In most CTD and Cyber cases and all CD cases, we follow the October 31, 2003 AG Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG)

[redacted]

National Security Undercover Operations

- Follow the NFIP Manual.
- [redacted]
- Specifically [redacted]
- [redacted]
- If sensitive circumstance, the [redacted] JCOs [redacted] and Assistant Director

Group I [redacted] (Sensitive Circumstances)

- Listed under [redacted]
- Involvement of [redacted] government officials, religious organizations, political organizations, or news media
- Utilization of a proprietary
- Utilization of an extraordinary technique [redacted] (mail cover)

b7E

~~SECRET~~

~~SECRET~~

b7E

Group I [redacted]
(Sensitive Circumstances)

Joint [redacted] with another member of the US Intelligence Community or a foreign intelligence service

- Significant questions of law or policy, e.g., civil liability, entrapment, otherwise illegal activity, or danger to UC Agent or others
- Expenditures over the \$100,000 cumulative maximum funding level - approved by [redacted]

Group II [redacted]

- Approved by SAC (initial proposal must have FBIHQ concurrence) for up to two six-month periods.
- Cumulative Spending Authority of \$100,000 (Initial + 1 renewal).
- Group IIs extending beyond the initial two six-month periods may be re-authorized by the Assistant Director or a Deputy Assistant Director in CD, CTD or Cyber

[redacted]

b7E

[redacted] s. Proprietary (S)

[redacted]

- If FBI paying start-up costs (e.g., lease space, pay for equipment) then probably have FBI business = PROPRIETARY

[redacted]

Criteria for National Security UC or (S)

[redacted]

- Initially ensure that ...

[redacted]

Make sure you have a foreign power

Other considerations

- Follow NSIG
 - Before consensual monitoring
 - Before interviewing
- MOUs/LOEs with other agencies
- Non-disclosure agreements/PSAs
- Coordination/concurrence of other agencies

[redacted]

b1
b7E

Attorney General Exemptions

- Lease or buy real estate/apartment, etc. (if month-to-month, no exception needed - cannot exceed 6 months and cannot go into next fiscal year).
- Deposit appropriate funds in a joint bank account.
- Utilize operational proceeds to offset expenses, and
- Establish an FBI proprietary business (if holding business out to public, seek exemption)

AG Exemption request should be coordinated with NSLB.

AG Exemptions - Proprietary

- Limitations on FBI's ability to operate communications proprietary
- No FBI-operated websites, telephones, etc. - accessible to public
 - Except for baskettapping
 - Possible exception if significant target
 - Innocent image-type ops allowed - public access chat rooms
 - Asset ops ok - but keep limits on FBI activity in mind
- Internet forum - if not accessible to general public (password protected), then not proprietary

[redacted] if no other sensitive circumstance as in [redacted]

Legal Considerations for Internet Operations

- Undisclosed participation
- Non-disclosure issues
- Operational (computer) security - need for lease space exemption
- Consensual monitoring/court orders
- Otherwise illegal activity
- Entrapment
- Extraterritorial activity
- First Amendment

b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

(S)

[Redacted]

[Redacted]

[Redacted] issues

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

- Advisable to house computer equipment at site not related to FBI.
- To lease space - will likely need AG exemption, so allow enough time to obtain from DOJ.

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

NSLB: Otherwise Illegal Activity

- DOJ 1988 MEMO for intelligence and counterterrorism-intel related requests (w/ an emergency exception)
 - Through [Redacted]
- U.S. Attorney letter supporting said UCO if criminal matter.

[Redacted]

b7E

(S)

Entrapment

- Same principles apply in national security matters to be prosecuted as in criminal cases
- Avoid government inducement and need predisposition on part of target, so be careful in how UCE interacts with target
- Any questions, ask prosecutor, ILU, NSLB

(S)

OVERSEAS ACTIVITIES IN UCOs

The AG Guidelines for National Security Investigations & Foreign Intelligence Collection apply.

Need DCI Concurrence and AD approval (although delegated to DADs and SC in 1994)

[Redacted]

First Amendment

- Avoid targeting simply because of protected speech
 - Follow NSIG
- Avoid posting inciteful material - e.g., how to make an explosive device

[Redacted]

b1
b7E

~~SECRET~~

~~SECRET~~

Undercover Team



UCO Proposal



After Approval of UCO



b7E

QUESTIONS?

• National Security Law Branch

- SSA [redacted]
- AGC [redacted]
- CI [redacted]
- SSA [redacted]
- SSA [redacted]
- MAPA [redacted]

b6

b7C

b7E

~~SECRET~~

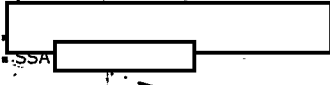
~~SECRET~~

DATE: 02-05-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-05-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence Undercover Operations



Outline

- History of FBI Undercover
- Terms of Reference
- Developing an Operation
- Practical Exercise
- Support for UCOs
- Review

7/10/2011

~~SENSITIVE~~

The History of Undercover Operations in the FBI

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



7/10/2011

~~SENSITIVE~~

b6
b7C
b7E

The History of Undercover Operations in the FBI

- Special Intelligence Service Division, 1940 - 1946
- Conducted Counterespionage, Counter-Sabotage, and Foreign Intelligence Operations in Latin America.
- Dissolved in 1946 with the establishment of the Central Intelligence Group (later CIA)



7/10/2011

~~SENSITIVE~~

The History of Undercover Operations in the FBI - Current Era

- Renewed emphasis in Criminal Investigations beginning in 1972
- 25 Special Agents from the Northeast offices
 - Targeted Organized Crime & Public Corruption
- Domestic Security and Counterintelligence UCOs
 - Less Well Known



7/10/2011

~~SENSITIVE~~

Terms of Reference

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

7/10/2011

~~SENSITIVE~~

b7E
b6
b7C

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 USC 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.

7/10/2011

~~SENSITIVE~~

Terms of Reference

- Undercover Operation



7/10/2011

~~SENSITIVE~~

Terms of Reference



7/10/2011

~~SENSITIVE~~

b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

Terms of Reference

- Group I [redacted]
 - Involve Sensitive Circumstances, Requiring FBIHQ Review and Oversight
 - Reviewed by the [redacted]
 - Subject to Annual On-Site Review
 - FBIHQ funded up to \$2 million per year with AG exemptions.

7/10/2013

~~SENSITIVE~~

10

Terms of Reference

- Group II [redacted]
 - Approved by SAC/ADIC [redacted]
 - JACB 10-days to [redacted] and [redacted]
 - Reviewed by [redacted] and NSLB
 - One Renewal Under ADIC/SAC Authority
 - Subsequent Renewals by Assistant Director
 - Or upgrade to a Group I [redacted]

7/10/2013

~~SENSITIVE~~

11

Sensitive Circumstances

(1 of 3)

- Targeting Public Officials, Foreign Government Officials, Religious or Political Organizations, or News Media
- Significant Intrusion Into Legitimate Government Operations
- Proprietary Business - a sole proprietorship, partnership, corporation, or other business entity operated on a commercial basis, which is owned, controlled, or operated wholly or in part on behalf of the FBI, and whose relationship is concealed from third parties.
- Otherwise Illegal Activity

7/10/2013

~~SENSITIVE~~

12

b7E

Sensitive Circumstances

(2 of 3)

- Professional/ Confidential Relationships/ Privilege
- Significant Risk of Government Liability
- Risk of Danger to UCE or Others

[redacted]

7/10/2013

~~SENSITIVE~~

13

Sensitive Circumstances

(3 of 3)

- Significant Entrapment Issue
- Joint Operations with USIC or Foreign Intel Service
 - Includes Police Services responsible for National Security Matters
- Use of Extraordinary Techniques

[redacted] ELSUR, Special Projects

7/10/2013

~~SENSITIVE~~

14

Developing an Operation

7/10/2013

~~SENSITIVE~~

15

b7E

What Exactly is Undercover?

- Involves building relationships
 - Rapport, Not Coercion
- Subsequent betrayal of these relationships in most cases.
- May not be Overt

[redacted]

- Not proper for all investigations
 - Saye'it for Priority Targets

7/10/2013

~~SENSITIVE~~

16

Why Have a UCO?

- Direct Contact Required to Achieve Investigative Goals
- UCE understands FBI intelligence collection requirements.

7/10/2013

~~SENSITIVE~~

17

Considerations

- It is a Team Effort
- Can Your Office Support the Op?
- Do You Have the Bench?
- Personnel - Case Agent, Co-Case Agent, UCE, Accountant, Intelligence Analyst, Contact Agent.

7/10/2013

~~SENSITIVE~~

18

b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

Objectives

- Intelligence for National Policymakers
- Collect-CT [redacted] CT [redacted]

7/16/2001 ~~SENSITIVE~~ 19

Initiation/Coordination Process

- Develop a Concept of the Operation
 - Beginning, Middle, and End
 - FD-997
- Field Coordination
 - SSA, UCC, CDC, & [redacted]
- HO Coordination
 - [redacted] NSLB

7/16/2001 ~~SENSITIVE~~ 20

Fundamentals

- Identify the Target [redacted] required
 - Is it a [redacted]
 - Does it Warrant the Resources?
- Identify the Objectives
 - Overall
 - Near Term (Six Months) [redacted]
- Discuss with the [redacted]
 - Do They Support the Operation?
 - Is it Consistent with the Strategic Plan?

7/16/2001 ~~SENSITIVE~~ 21

Know the Target

- Seek the Advice of Professionals
 - Behavioral Analysis Program
- What Can Behavior Tell Us?
 - How We Build a Relationship
 - How We Will Betray It
 - Or How He Will Betray Others
 - Needs = Vulnerabilities

7/16/2001 ~~SENSITIVE~~ 22

Selecting a UCE

- Certification
 - Required for Primary Roles
- Case Specific Authority for Non-Certified Employees
 - AD Authority
 - Limited Roles

7/16/2001 ~~SENSITIVE~~ 23

Support for UC Activities & Operations

- Field Office UC Coordinator
 - Local Subject Matter Expert
 - [redacted] Contact
- Coordination & Oversight
 - Operational & Administrative Training
- Behavioral Analysis Program
 - Especially in [redacted]

7/16/2001 ~~SENSITIVE~~ 24

b7E

Support for UC Activities & Operations

- [redacted]
- [redacted]

7/16/2001 ~~SENSITIVE~~ 25

Support for UC Activities & Operations

- [redacted] of UCEs
- Prior to Training & Certification
 - Even for Case-Specific Authority
 - Even for "Five Contacts"
- Pre-Operational
- Mid-Operation
 - Every Six Months
- Post-Out

7/16/2001 ~~SENSITIVE~~ 26

Resources and References

- Domestic Investigations and Operations Guide
- Counterintelligence Program Guide
- NFIPM Section 28, Undercover Operations
- Field Guide to Undercover and Sensitive Operations
- Confidential Funding Guide
- Field Office Undercover Coordinator
- [redacted] Regional

7/16/2001 ~~SENSITIVE~~ 27

b7E

~~SECRET~~

~~SECRET~~

b6
b7C

Points of Contact

Region	Primary Program Manager	Secondary Program Manager
North	[REDACTED]	[REDACTED]
Northwest	[REDACTED]	[REDACTED]
Southwest	[REDACTED]	[REDACTED]
West	[REDACTED]	[REDACTED]
Central	[REDACTED]	[REDACTED]
South	[REDACTED]	[REDACTED]
OGC/NSLR	[REDACTED]	[REDACTED]
AGC	[REDACTED]	[REDACTED]
SSA	[REDACTED]	[REDACTED]
AGC	[REDACTED]	[REDACTED]
SS	[REDACTED]	[REDACTED]

7/12/2011 ~~SECRET~~

Program Managers by Region

Region	Primary Program Manager	Secondary Program Manager
North	[REDACTED]	[REDACTED]
Northwest	[REDACTED]	[REDACTED]
Southwest	[REDACTED]	[REDACTED]
West	[REDACTED]	[REDACTED]
Central	[REDACTED]	[REDACTED]
South	[REDACTED]	[REDACTED]
OGC/NSLR	[REDACTED]	[REDACTED]
AGC	[REDACTED]	[REDACTED]
SSA	[REDACTED]	[REDACTED]
AGC	[REDACTED]	[REDACTED]
SS	[REDACTED]	[REDACTED]

7/12/2011 ~~SECRET~~

b6
b7C
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Undercover Activities &
Operations for Foreign
Counterintelligence

Basic Counterintelligence
Operations Course for
Special Agents

7/15/2010 ~~SENSITIVE~~ 1

Outline

- Terms of Reference
- Why a UCO
- Conducting UC Activities & Operations
- Support for UC Activities & Operations
- Coordination for UC Activities & Operations
- Considerations in Planning UC Activities & Operations

7/16/2011 ~~SENSITIVE~~ 1

Terms of Reference

- Undercover Employee
 - Any Special Agent, Support Employee, Task Force Agent of Officer, or other person (excluding Assets), acting at the behest of the FBI in the conduct of Undercover Activities.

7/16/2011 ~~SENSITIVE~~ 2

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 in substantive contacts with the target of an FBI investigation. Such activities may include contacts with targets of opportunity when continued contact is not anticipated.

7/16/2011 ~~SENSITIVE~~ 3

Terms of Reference

- Undercover Operation

7/16/2011 ~~SENSITIVE~~ 4

Terms of Reference

b7E

7/16/2011 ~~SENSITIVE~~ 5

Terms of Reference

- Undercover Operation
 - Involve Sensitive Circumstances, Requiring FBIHQ Review and Oversight, or
 - Funding in Excess of ADIC/SAC Authority
 - Reviewed by the [redacted]

7/16/2011 ~~SENSITIVE~~ 6

Sensitive Circumstances
(1 of 3)

- Criminal - Investigations of Public Officials - Significant Intrusions Into Legitimate Govt Opns - Proxies - Otherwise Illegal Activity (OIA)	- National Security - Targeting Public Officials, Foreign Govt Officials, Religious or Political Organizations, or News Media - Significant Intrusions Into Legit Govt Opns - Proxies - OIA
--	--

7/16/2011 ~~SENSITIVE~~ 7

Sensitive Circumstances
(2 of 3)

- Criminal - Professional/Confidential Relationships/Privilege - Significant Risk of Govt Liability - Risk of Violence - Risk of Financial Loss	- National Security - Professional/Confidential Relationships/Privilege - Significant Risk of Govt Liability - Risk of Danger to UCE or Others
--	---

7/16/2011 ~~SENSITIVE~~ 8

~~SECRET~~

~~SECRET~~

Sensitive Circumstances
(3 of 3)

- Criminal
 - Providing Instrumentalities of the Crime
 - Risk of Arrest and False Testimony
- National Security
 - Significant Entrapment Issue
 - Joint Opns with USIC or Foreign Intel Service

7/18/2011 ~~SENSITIVE~~ 10

What Exactly is Undercover?

- Involves building relationships
 - Rapport, Not Coercion
- Subsequent betrayal of these relationships in most cases.
 - May not be Overt

7/18/2011 ~~SENSITIVE~~ 11

Why Have a UCO

7/18/2011 ~~SENSITIVE~~ 12

b7E

(S)

Objectives

- Criminal
 - Evidence for Prosecution
 - To Determine If a Full Investigation is Warranted
 - Prevent, Solve, and Prosecute General Crimes
 - Ascertain Scope of Racketeering and Terrorism Enterprises
- National Security
 - Intelligence for National Requirements

7/18/2011 ~~SENSITIVE~~ 13

Conduct of UC Activities & Operations

- Define the Target
 - Predicated Subject
- Conduct Logical Investigation
 - Do the Homework to Ensure Success
 - Is UC Activity/Operation Appropriate?
- Define Objectives
 - Overall
 - Short-term
- Develop a [redacted]

7/18/2011 ~~SENSITIVE~~ 14

Support for UC Activities & Operations

- Field Office UC Coordinator
 - Local Subject Matter Expert
 - Facilitate Coordination
- FBIHQ [redacted]
 - Coordination & Oversight
 - Operational & Administrative Training

7/18/2011 ~~SENSITIVE~~ 15

b1
b7E

Support for UC Activities & Operations

- Regional [redacted]

7/18/2011 ~~SENSITIVE~~ 16

Support for UC Activities & Operations

- [redacted] of UCEs
 - Prior to Training & Certification
 - Even for SAC Certified
 - Pre-Operational
 - Mid-Operation
 - Every Six Months
 - Post-Out

7/18/2011 ~~SENSITIVE~~ 17

Coordination of UC Activities & Operations

- Substantive Desk
 - Consistent with Program Strategies
- Field Office Undercover Coordinator
 - Advise & Assist With UC Matters
- Regional [redacted]
 - [redacted] UCEs

7/18/2011 ~~SENSITIVE~~ 18

b7E

~~SECRET~~

~~SECRET~~

Coordination of UC Activities & Operations

- OGC, National Security Law Branch
 - Legal Issues
 - Supplements the Review of Your CDC
- CD [redacted] Manager
 - Synchronization & Deconfliction

7/10/2011

~~SENSITIVE~~

30

Considerations

- Plan for Success
 - Anything Worthwhile Will Take More than Five Meets
 - And Rises to a Group I - Eventually

7/10/2011

~~SENSITIVE~~

31

Considerations

- [redacted]
 - Drafts to Substantive Desk and [redacted]
 - Finals to [redacted] ten Days Out

7/10/2011

~~SENSITIVE~~

31

b7E

Considerations

- It is a Team Effort
 - Case Agent
 - Case Accountant
 - Contact Agent
 - UCE
 - IA/Reports Officer
- Can Your Office Support the Op?
 - Do You Have the Bench?

7/10/2011

~~SENSITIVE~~

32

Considerations

- UCE
 - [redacted]
- Term Limits for Fulltime
 - Three Years (With One Year Extensions)
- Transfers
 - Needs of the Bureau

7/10/2011

~~SENSITIVE~~

33

Resources and References

- NSIG
- NFIPM Section 28
 - [redacted]
- Field Office Undercover Coordinator
 - [redacted]
- FBIHQ UC Program Manager
 - [redacted]

7/10/2011

~~SENSITIVE~~

34

b7E

Questions?

7/10/2011

~~SENSITIVE~~

35

Points of Contact

- [redacted]
 - SSA [redacted]
 - SSA [redacted]
 - SSA [redacted]
- NBSU
 - UC [redacted]
- OGC/NSLB
 - AGC [redacted]

7/10/2011

~~SENSITIVE~~

36

b6
b7C
b7E

~~SECRET~~

DATE: 02-07-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-07-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Overseas Operations



Overseas Operations

- Obtain Travel Documents
- Obtain Field and HQ approval

(S)

[Redacted]

[Redacted]

- Obtain AG Authority
- Pass security clearances
- Notify SIOC / Security Officer

[Redacted]

7/15/2011

~~SECRET~~//NOFORN

2

b1
b7E

Overseas Operations

- What are your objectives?
 - Liaison • Surveillance
 - Interview • Technical
- What do I bring?
 - Travel docs, paperwork, equipment, \$\$
- What authority do you need?
- Who are you asking for help?
 - LEGAT [Redacted] DOJ, locals

(S)

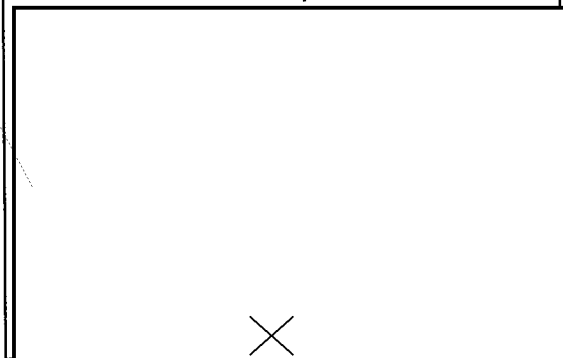
7/15/2011

~~SECRET~~//NOFORN

3

(S)

Overseas Operations



b1
b7E

Overseas Operations

- Resources [Redacted]
 - [Redacted] CC NETDM
 - [Redacted]
 - [Redacted]
 - [Redacted]
- Safety/Security
- Checklist for overseas travel

(S)

7/15/2011

~~SECRET~~//NOFORN

5

b1
b7E

~~SECRET~~

DATE: 02-13-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-13-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~



OSIC [redacted]

Unit Chief [redacted]

[redacted]

Counterintelligence Division

~~SECRET~~

~~SECRET~~

[redacted] Mission:

Establishment that CI and CTN efforts are made by facilitating and coordinating the efforts of the FBI and its U.S. Intelligence Community (USIC) partners in collecting Foreign Counterintelligence (FCI), Counterterrorism (CT), and Foreign Intelligence (FI) information in the U.S. against targets approved by the U.S. Foreign Intelligence Surveillance Court (FISC) and/or the Attorney General in support of both establishment and non-establishment offices and the our USIC partners.

• Provide Program Management for all [redacted] programs to include oversight of [redacted]

~~SECRET~~

~~SECRET~~

[redacted] Mission Simplified:

- Customs Interdiction [redacted]
- DOE Initiative
- Operational Support to the Intelligence Community (OSIC) [redacted]
- Special Projects

~~SECRET~~

b7E

~~SECRET~~

[redacted] Liaisons

- Intelligence Community Partners [redacted]
- BOO Of [redacted]
- Contractors & Vendors [redacted]
- Other FBI Units [redacted]
- NSLB [redacted]
- OIG/ERP [redacted]

~~SECRET~~

~~SECRET~~

Customs Program

[redacted]

[redacted]

• Every search conducted under this program must be coordinated through [redacted]

~~SECRET~~

~~SECRET~~

[redacted]

- Provides Operational Support to the Intelligence Community (OSIC)
- [redacted]

~~SECRET~~

b7E

~~SECRET~~

[redacted]

[redacted]

[redacted]

~~SECRET~~

~~SECRET~~

OSIC

- EO 12333
- Covert collection platforms
- Close access operations
- Supply Chain Interdiction
- Multiple sources of funding

~~SECRET~~

~~SECRET~~

[redacted]

~~SECRET~~

b7E

~~SECRET~~

AC/LURM042951

~~SECRET~~

b1
b7E

(S)

~~SECRET/NOFORN~~

Special Projects:

- Extraordinary Technology
- Deployed Covertly
- Covert Collection
- Against CD/CTD Targets
 - Human
 - Establishments



~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Extraordinary Technology:



~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Construction Programs:

- Special Project technology
- Deployed Covertly
- During Construction/Renovations



~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

SP vs. Traditional Technology

Traditional	Special Projects
• Funded technical field support and services.	• Funded by dedicated Technical Program.
• Equipment resides in the field.	• Equipment generally resides at HAF.
• Technology unclassified.	• Classified Secret/TC.
• Legal Authority req'd.	• Legal Authority req'd.
• Field Division has approval authority.	• HAFIR, SPAB approval required.

~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Reasons to use Special Projects

- Limited Access and/or Egress to target.
- Strong TSCM capabilities of target.
- Politically sensitive target.
- Potential loss of life/grave injury/serious property damage.



~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Special Project Process

- Identify the Opportunity (Field)
- Gather the required information (Field)
- Develop a Plan (Field w. [redacted])
- Present your plan by way of EC & Form
- SPAB approval [redacted] Advisory Board)
- Deployment (Field + HQ + OTD)
- Post Deployment (Field + HQ + OTD)

~~SECRET/NOFORN~~

b7E

~~SECRET/NOFORN~~

Special Project Team

- The Case Agent
- The Field Technically Trained Agent
- The OTD Engineer
- The [redacted] Program Manager
- The HQ Substantive Program Manager

~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Special Project Initiation

- Steps to initiate a Special Project
 - Identify the potential opportunity
 - Contact with [redacted] Early
 - Complete a Special Project Request EC
 - Complete a Special Project Request Form
 - See [redacted]
 - Forms and Ponies
 - Special Project Guidance

~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

Special Project Request Form & EC

- Identify the Target (Specificity)
- Substantive Case File
- Technique requested (No need to explain technique)
- Operational need/Brief Case Summary
- Current technical coverage in place
- # of IIRs produced from current coverage
- Relevant [redacted]
- Window of Opportunity/Deployment date
- Operational Plan

~~SECRET/NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~
Special Project Initiation

- Description of expected intelligence
- Collection Requirements to be addressed
- [redacted] to be filled
- LP status (if applicable)
- Field Manning (# of agents, analysts, linguists)
- [redacted]
- NFPO status (When last issued)
- Completely filled out
- All required signatures

~~SECRET~~
Special Project Process

- Identify the Opportunity (Field)
- Gather the required information (Field)
- Develop a Plan (Field w/ [redacted])
- Present your plan by way of EC & Form
- [redacted] & Advisory Board)
- Deployment (Field + HQ + OTD)
- Post Deployment (Field + HQ + OTD)

~~SECRET~~
Special Project Process

- [redacted] Preparation
- [redacted] report
- Technical / Operational plan
- Cost Analysis
- Risk Analysis provided by [redacted]
- FISA Review with NSLB
- NFPO Review with [redacted]
- [redacted]
- [redacted]

b7E

- ~~SECRET~~
- Presented by [redacted] SSA
 - Chaired by the CD/CTD Deputy Assistant Director
 - Board Membership:
 - [redacted] Chief
 - [redacted] Chief
 - [redacted] Section Chief
 - [redacted] Unit Chief
 - OSC/NSLB
 - Analytical Section Chief
 - Representation by [redacted] necessary

~~SECRET~~
Special Project Process

- Special Project Approved (Caveats?)
- Obtain/modify FISA authority (HQ only)
- AG Exemptions for covert accounts, lease of property, etc [redacted]
- Coordination with other USIC agencies [redacted]
- Entry notification through [redacted]

~~SECRET~~
Special Project Process

- Identify the Opportunity (Field)
- Gather the required information (Field)
- Develop a Plan (Field w/ [redacted])
- Present your plan by way of EC & Form
- [redacted] approval [redacted] Advisory Board)
- Deployment (Field + HQ + OTD)
- Post Deployment (Field + HQ + OTD)

b7E

~~SECRET~~
Special Project Deployment:

- [redacted] notifies field of [redacted] approval
- [redacted] sends approval EC
- OTD and the Field coordinate deployment

~~SECRET~~
Special Project Post Deployment:

- Field Provides Quarterly Reports to [redacted]
- Monitor for future opportunities

b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

~~SECRET~~

CONTACTS

Counterintelligence Division

OSIC

~~SECRET~~

~~SECRET~~

Questions



~~SECRET~~

b7E

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET//NOFORN~~



CI -Cyber Investigations

A New Threat
A New Frontier
(Not really)

SSA

FBI Counterintelligence
Training Center (CITC)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



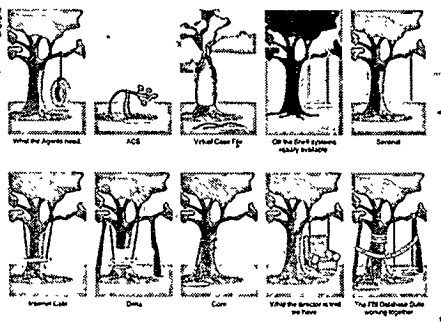
FBI Next Generation Workstation



~~SECRET//NOFORN~~

b6
b7C

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Key Concepts

- What is a CI-Cyber Investigation
- Why do we care
- Where is the battle fought
- Who is fighting it
- How do you work a CI-Cyber investigation
- Resources and References

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



What is a CI-Cyber Investigation?

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~



Why do we care?

- "The hacker can steal information from the enemy to understand his operational channels; alter information in his orders, causing the enemy to follow orders that he himself issued; delete critical data from the enemy's data base; or damage systems in the enemy command control center or installed in high-technology weapons."

2006 edition of The Science of Campaigns, published by the PLA's National Defense University



~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

And...

■ *"The most complex and at the same time most effective form of [information] aggression is a purposeful effect on the process of preparing a decision in states' command and control structures by introducing additional data or disinformation to them."*

-Russian MGen



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Cyber uses in ground conflicts

■ Georgia:

- Disinformation During Conflict (August 2008)
- National Bank of Georgia (NBG) hacked
- Added a script advising customers will not have access to [redacted] due to the military conflict.

[redacted]

~~SECRET//NOFORN~~

b7E

~~SECRET//NOFORN~~

A glimpse into the future?

■ (U) Data Theft Surpasses Physical Losses as Biggest Problem for Global Companies

- (U) According to the Kroll annual global fraud survey, more than 27 percent of the 801 global companies surveyed reported data losses this year, up from 8 percent last year.
- (U) China has become the single most problematic market for multinationals; 98 percent of corporations that do business there reported some sort of fraud loss, up from 6 percent a year ago.
 - (U) Source: Financial Times
 - (U) No associated cases identified.

10/18/10 Cyber Intelligence Executive Daily Brief

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Some real dangers

- The adversary can develop an in-depth knowledge of our networks
- Persistent and apparently legitimate network presence
- Operational or Real-Time Data theft from Networks

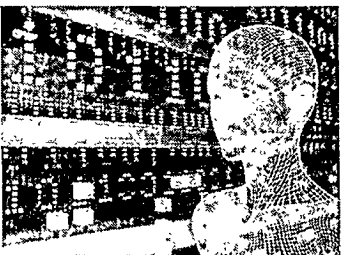
(S) [redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

How do we address it?



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Key Goal of the CI Investigator

Cyber techniques are just a sophisticated form [redacted]

HOWEVER [redacted]

Behind every intrusion is a person or set of persons.

~~SECRET//NOFORN~~

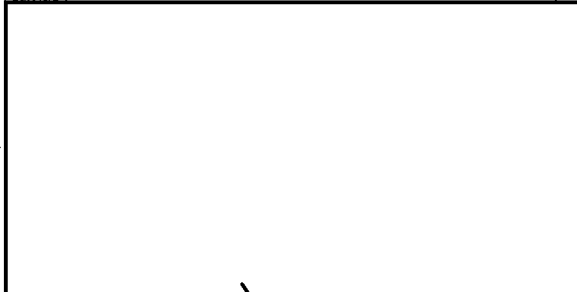
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

A Joint Cyber/CI Effort



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

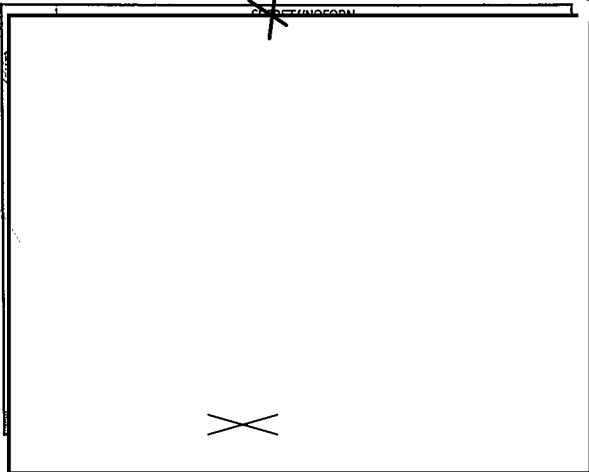
CI and Cyber
Working together to stick it to
the bad guy.



~~SECRET//NOFORN~~

b7E
b1

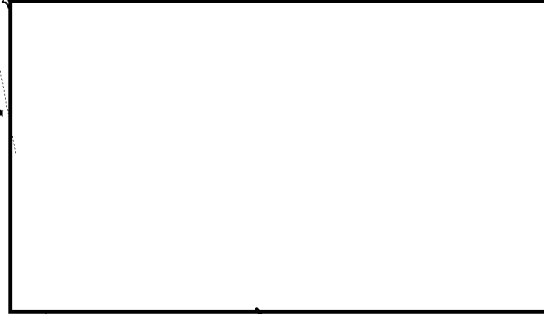
~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Who is on the front line of the
CI-Cyber war?



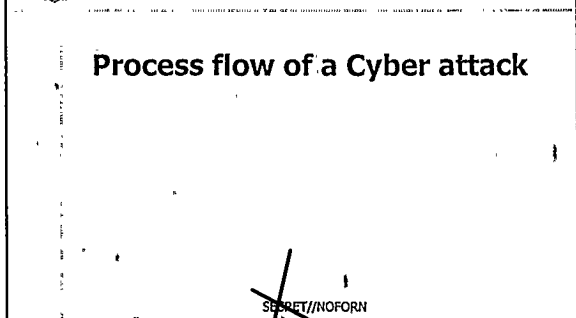
~~SECRET//NOFORN~~

b7E
b1

~~SECRET//NOFORN~~



Process flow of a Cyber attack

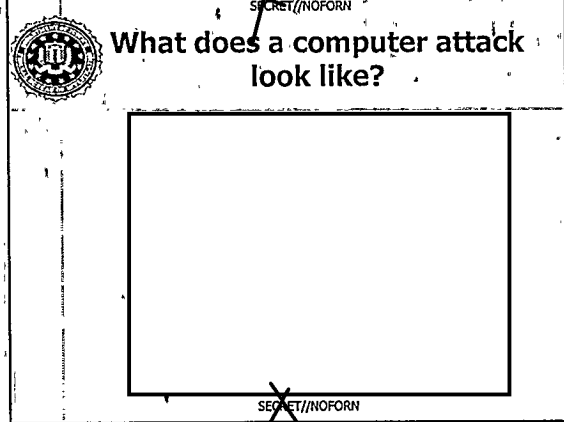
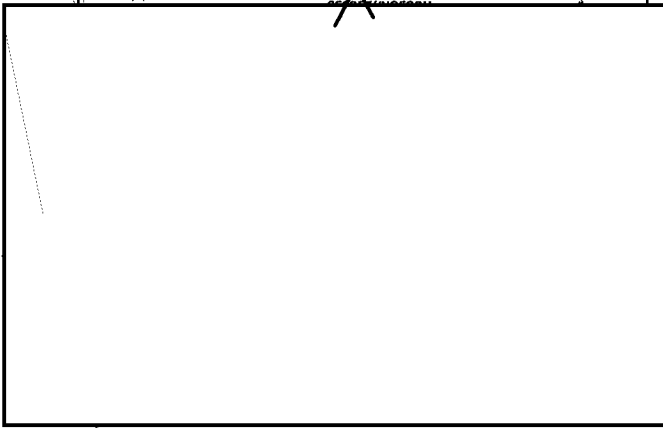


~~SECRET//NOFORN~~

~~SECRET~~

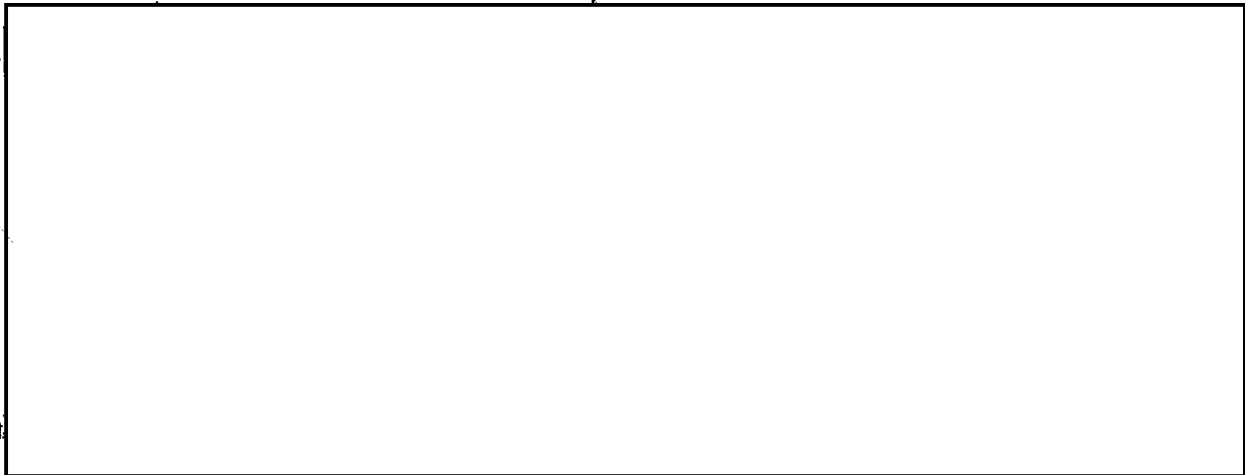
~~SECRET~~

(S)

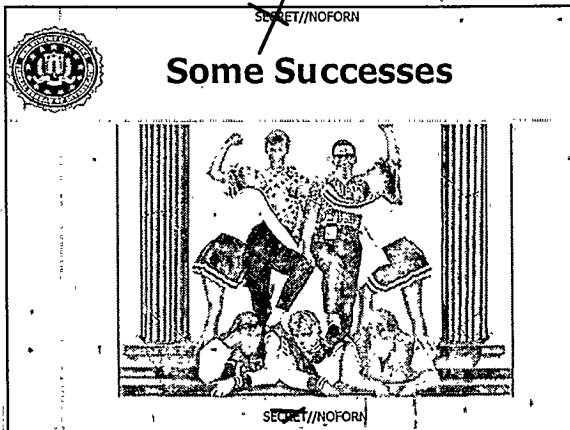


b1
b6
b7C
b7E

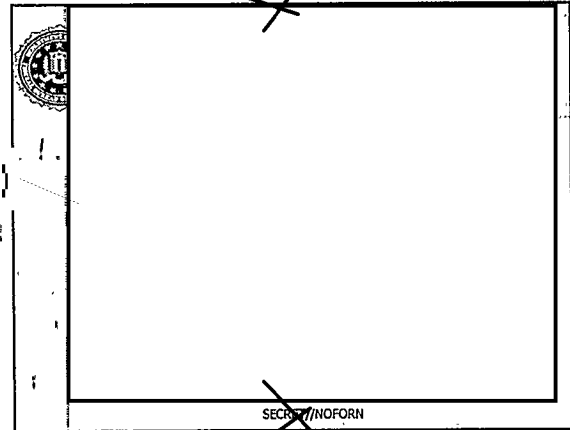
(S)



b1
b7E



(S)

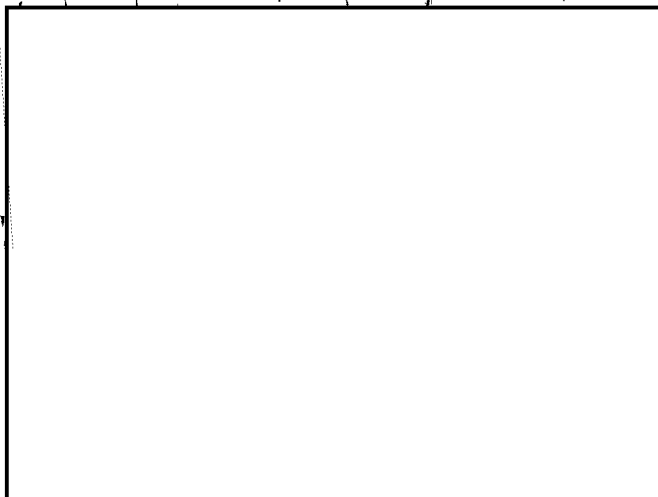
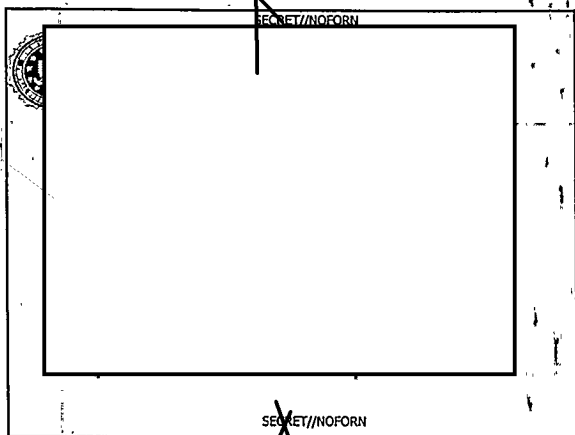


b1
b7E

~~SECRET~~

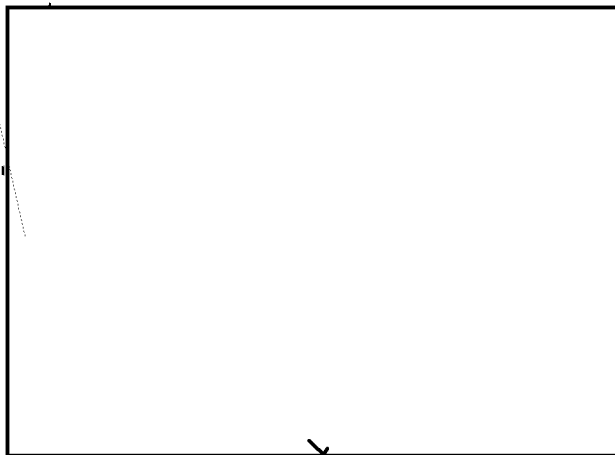
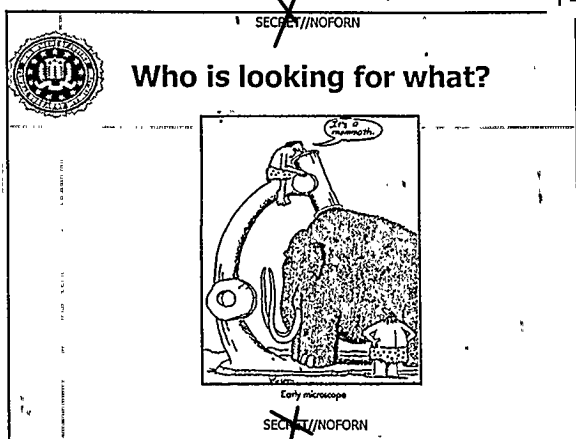
~~SECRET~~

(S)



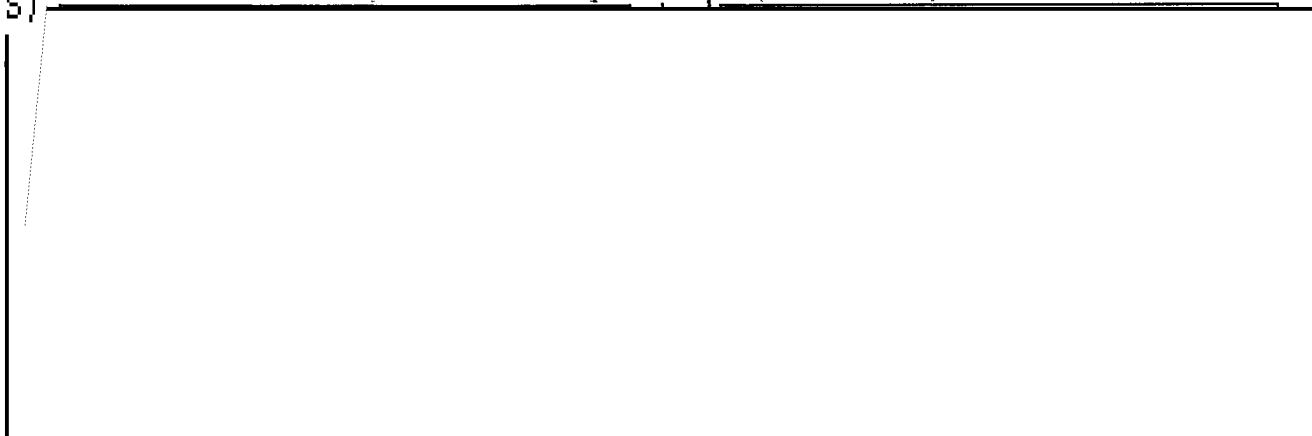
b1
b7E

(S)



b1
b7E

(S)



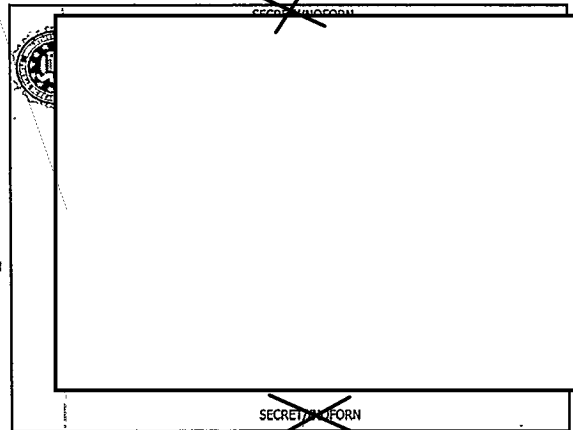
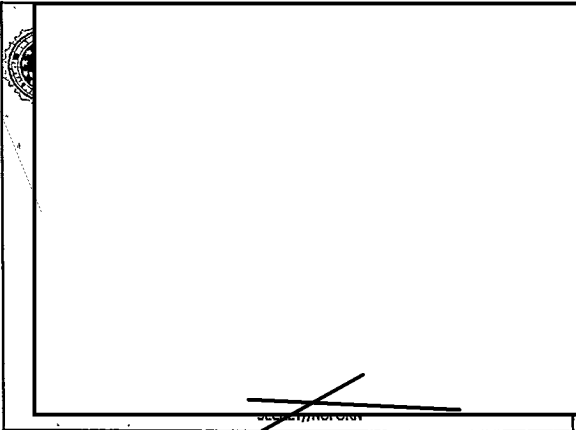
b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)



b1
b7E

~~SECRET//NOFORN~~



How to work a CI/Cyber Case



FAILURE
While there is no I in team, there is a U in failure.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Defining the Investigative Roles

- **Cyber's role:** evaluate the tools, techniques and procedures (TTPs)
- **CI's role:** evaluate the [redacted]
- CI & Cyber must work together to mitigate and exploit the threat

~~SECRET//NOFORN~~

b7E

(S)

(S)

(S)

~~SECRET//NOFORN~~



How to conduct a CI/Cyber Investigation

- Think like [redacted]
- Coord [redacted]
- There is no [redacted]
- Use imagination [redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~



How to conduct a CI/Cyber Investigation

[Large redacted content block]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

b1
b7E

~~SECRET//NOFORN~~

Cyber Questions to ask in a CI-Cyber Case

- IP address of victim
- IP address of attack (logs)
- ISP for victim
- Network / Firewall logs
- Machine logs
- Firewall: [redacted]

b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Data we can use *Bread Crumbs...*

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

What the Cyber Side can tell us

(S)

~~SECRET//NOFORN~~

"In the news..."

- Peer to Peer Ad-hoc wireless networks
- [redacted]
- Virtual meets (second life)
- Twitter
- Facebook [redacted]

b1
b7E

~~SECRET//NOFORN~~

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~



Speaking of Social Networks...

- Do not promote personal or professional importance in a profile or post
- Do not provide details about work/colleagues/position or duties
- Do not discuss government computer systems/weaknesses/vulnerabilities/loopholes
- Think before you post: Put it on a billboard?
- Limit who may contact you
- Friend or friend settings
- Picture data
- Limit Personal data

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



So what's this "Z" class anyway?

- CI investigation with Cyber [redacted]
- Sensitive end point victim [redacted]
- [redacted]
- Can start in either venue (CI or Cyber)
- Situation dictates (Depth of the invest)
- 203Z – Attribution less



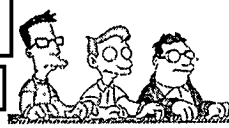
~~SECRET//NOFORN~~

b7E

(S) ~~SECRET//NOFORN~~



What can FBIHQ and NCIJTF (S) for you?



- Develop an awareness of CI/Cyber [redacted]
- Facilitate joint operations with other USG agencies.
- Training opportunities

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Counterintelligence POCs to NCIJTF

[redacted]

Matters

SSA [redacted]

SSA [redacted]

Global CI Matters

A/UC SSA [redacted]

[redacted] Matters

SSA [redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~



Security References

[redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



Risk Reduction

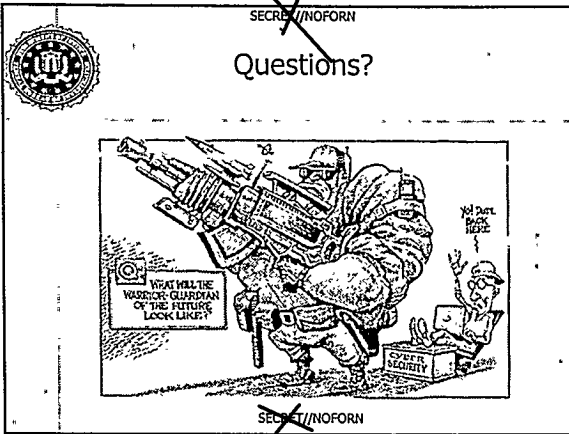
- Regular maintenance (patches)
- Hazardous World (adult, foreign)
- Anti-virus (Zero Day exception) (updates signatures, regular scans)
- Educated users (I love you, common sense-UPS)
- Close Common doors (default access)
- Forwarded emails (phishing)
- Disposable email accounts
- Good passwords

~~SECRET//NOFORN~~

b7E

~~SECRET~~

~~SECRET~~



~~SECRET~~

ACLURM042963

FBI041863

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

Introduction to Cyber CI
Investigations



~~SECRET~~
Derived From: G3
Declassify: X1

Federal Bureau of Investigation
Cyber Division - [redacted]
SSA [redacted]

~~SECRET/NOFORN~~

Consider this...



movement information from Defense Dept. computers and tried to sell it to Iraq, who thought it was a hoax and turned it down.

- ❑ In 1997-98 "Analyzer", an Israeli youth, tutored 2 CA teenagers and they (allegedly) hacked into Pentagon (The "Holy Grail" of hacking) and other US military computers.
- ❑ In March 1997, as a result of a series of commands sent from a hacker's PC, vital services to the FAA control tower in Worcester, MA were disabled for 4 hours.

~~SECRET/NOFORN~~

Why is this important??



~~SECRET/NOFORN~~

b6
b7C
b7E

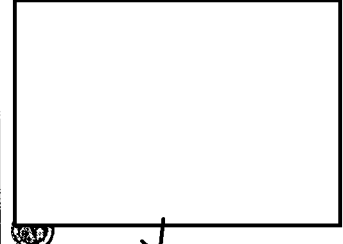
Critical Infrastructures
Services so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.



~~SECRET/NOFORN~~



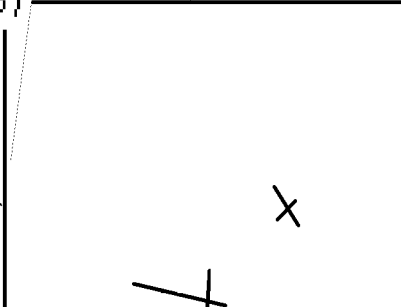
~~SECRET/NOFORN~~



~~SECRET/NOFORN~~

b7E

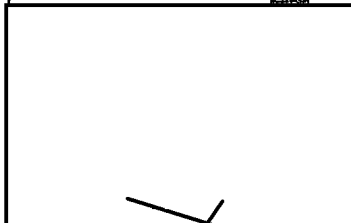
(S)



~~SECRET/NOFORN~~



Outages in [redacted]



~~SECRET/NOFORN~~

b1
b7D

~~SECRET~~

~~SECRET~~

b7E



Cyber Division (Created Fall 2002)

The Cyber Division (CyD) of the FBI was established to protect the United States against cyber-based attacks and high-technology crimes.



~~SECRET NOFORN~~

FBI Priorities:

1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. Protect the United States against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational and national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission

~~SECRET NOFORN~~

Cyber Division Mission:

Cyber Division is dedicated to applying the highest level of technical capital to understanding cyber-based terrorism, hostile intelligence operations conducted over the Internet, and cybercrime. By aggregating its cyber-centered investigations within one division, the FBI is able to more effectively and efficiently identify, investigate, and neutralize cyber threats. As the nation's cyber dependency becomes even more profound, the Cyber Division will continue to be the vanguard of security for its citizens and its critical infrastructures.

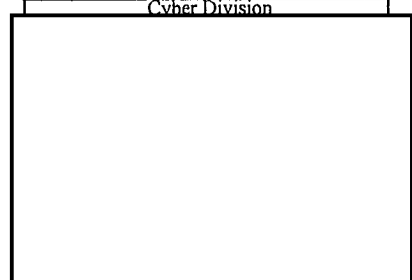
~~SECRET NOFORN~~

Cyber Division Priorities

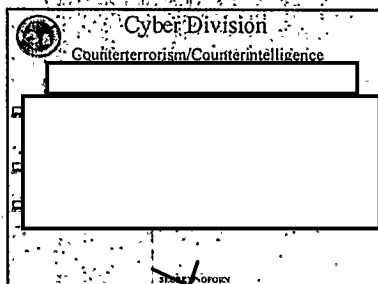
1. Cyber Terrorism
2. [Redacted]
3. Criminal Intrusions
4. Internet Issues
5. Intellectual Property
6. Internet Fraud

~~SECRET NOFORN~~

Cyber Division



b6
b7C
b7E



~~SECRET NOFORN~~

Computer Intrusion Section (CIS)

- 288B CI Computer Intrusion
- 288F CI Technical Support
- Cyber UCCs

~~SECRET NOFORN~~

CT/CI Intrusion Cases FY 2002 - 2006



FY 2002 FY 2003 FY 2004 FY 2005 FY 2006

~~SECRET NOFORN~~

b7E

~~SECRET~~

~~SECRET~~

CI Intrusion Investigation



- Deconfliction/Coordination with CD in the field office and at FBIHQ substantive desks.
- Technical Support to CI Program
- CI Investigation with cyber or IT nexus requiring the expertise of a trained cyber agent :
 - Reading e-mail headers
 - Obtaining Internet Protocol (IP) Information
 - Technical aspects of a UCO

~~SECRET/NOFORN~~

Why the Need for Deconfliction ?



- Growing number of Cyber/CI investigations
- Prevent duplicative efforts
- Enhances communications/awareness
- Leads to coordinated efforts
- Identify best practices
- Mandated by [redacted]

~~SECRET/NOFORN~~

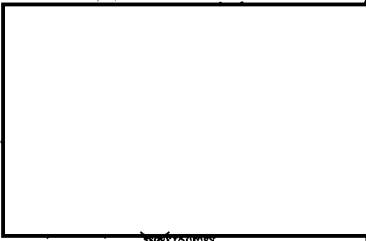
Why Cyber ???



~~SECRET/NOFORN~~

b7E

Why Computer Systems?: Cost & Means of Att ack



~~SECRET/NOFORN~~

Counterintelligence Division

How Cyber's Mission relates to CI's Mission:

- Prevent or neutralize the foreign acquisition of WMD or equipment;
- Prevent penetration of (the networks of) the US Intel Community, US Government, and contractors;
- Prevent the compromise of (the networks of) the [redacted];
- Conduct aggressive (Cyber) CI operations on most significant threat countries.

~~SECRET/NOFORN~~

(S)



U.S. National Intelligence Council/National Intelligence Estimate Cyber Threats to United States Information Infrastructure (January 2004) 6

~~SECRET/NOFORN~~

b1
b7E

(S)



U.S. National Intelligence Council/National Intelligence Estimate Cyber Threats to United States Information Infrastructure (January 2004) 6

~~SECRET/NOFORN~~

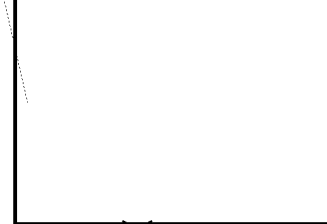
What kinds of Cases are we talking about ???



~~SECRET/NOFORN~~

(S)

Cyber CI cases



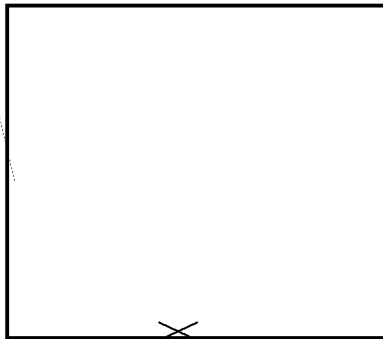
~~SECRET/NOFORN~~

b1
b7E

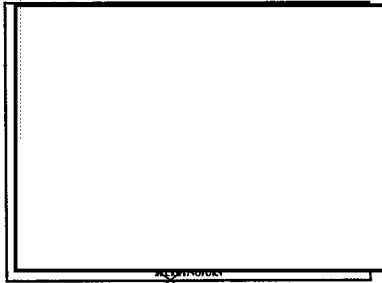
~~SECRET~~

~~SECRET~~

(S)



(S)



Washington Post April 14, 2005

- ☐ "China Operates the most extensive, technologically sophisticated and broad reaching system of internet filtering in the world"
- ☐ "The Chinese are successfully developing a market economy, at the same time they are continuing to accomplish control of the Internet"

b1
b7E

Washington Post April 14, 2005
Cont'd

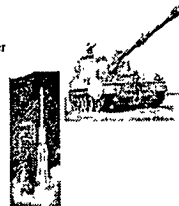
- ☐ "Chinese censorship claim as many as 30,000 Internet Police"



~~SECRET//NOFORN~~

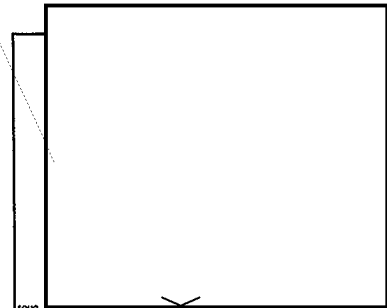
Washington Post April 12, 2005

- ☐ "India, China Hoping to Reshape the World Order Together"
- ☐ Pledge of New Strategic Alliance
- ☐ "If India and China Cooperate in the IT Industry, We Will Lead the World" (Chinese Premier Wen Jiabao)



~~SECRET//NOFORN~~

(S)

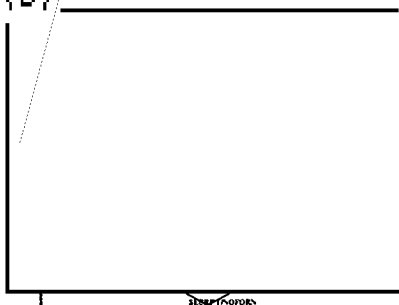


b1
b7E

(S)



(S)



(S)



U.S. National Intelligence Council//National Intelligence Estimate Cyber Threats to the United States Information Infrastructure//January 2004//S

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

U.S. National Intelligence Council//National Intelligence Estimate Cyber Threats to the United States Information Infrastructure//January 2004//S

~~SECRET//NOFORN~~

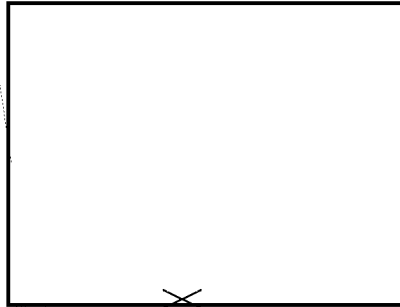
~~SECRET~~

~~SECRET~~

(S)

(S)

(S)



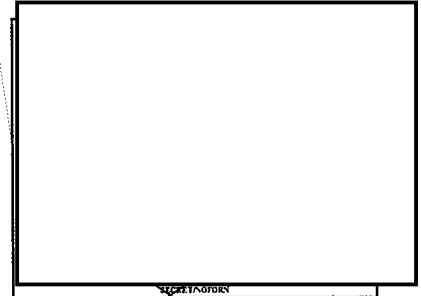
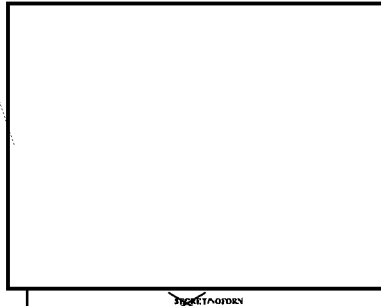
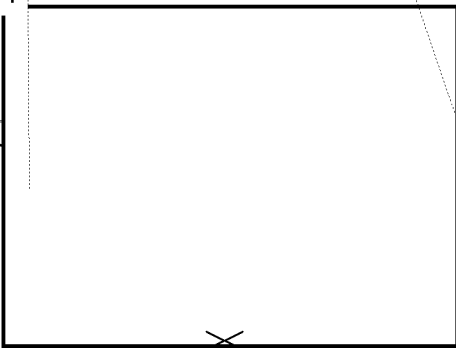
~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

(S)

(S)

(S)



~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

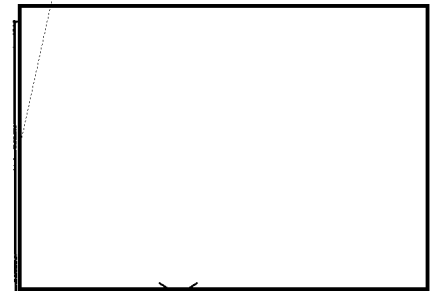
~~SECRET/NOFORN~~

b1
b7E

(S)

(S)

(S)



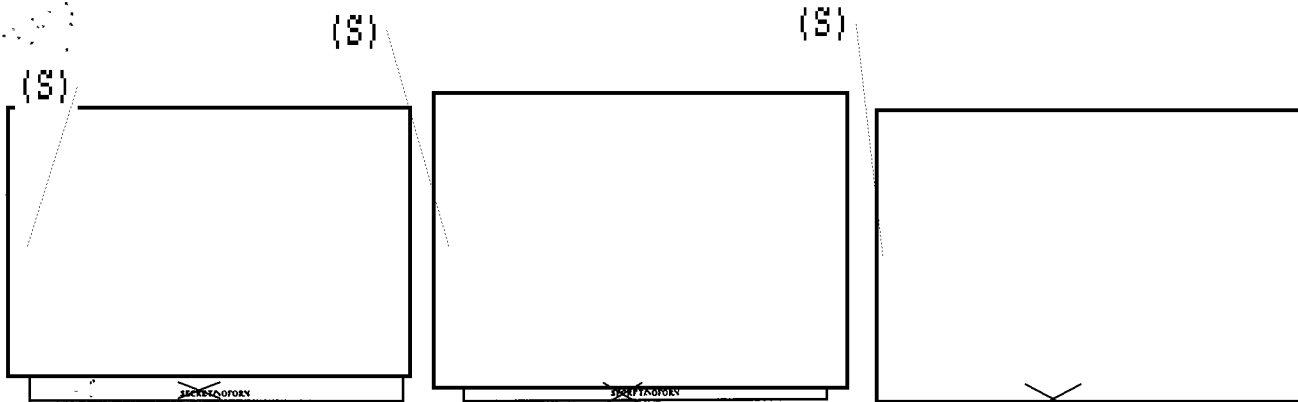
~~SECRET/NOFORN~~

~~SECRET/NOFORN~~

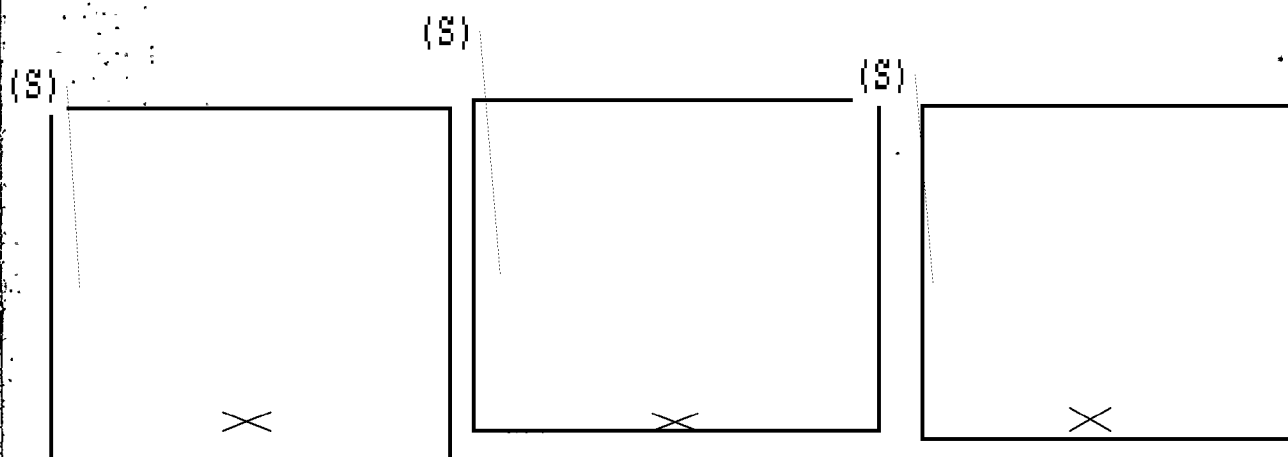
~~SECRET/NOFORN~~

~~SECRET~~

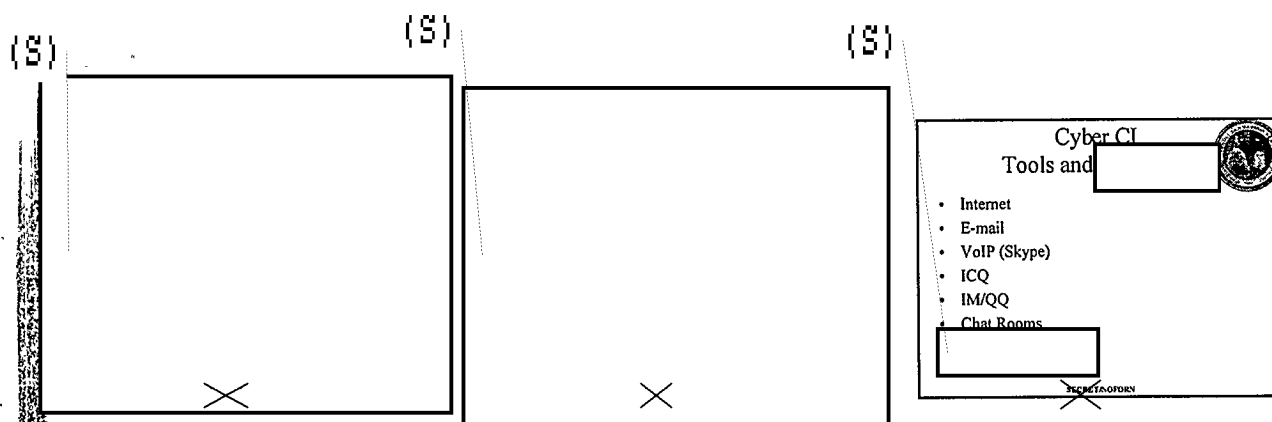
~~SECRET~~



b1
b7E



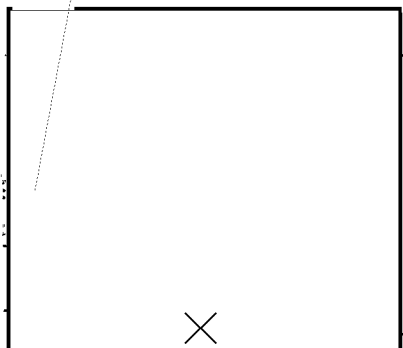
b1
b7E



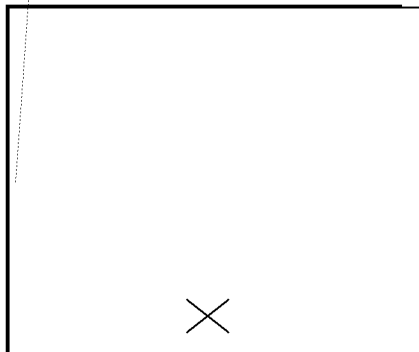
~~SECRET~~

~~SECRET~~

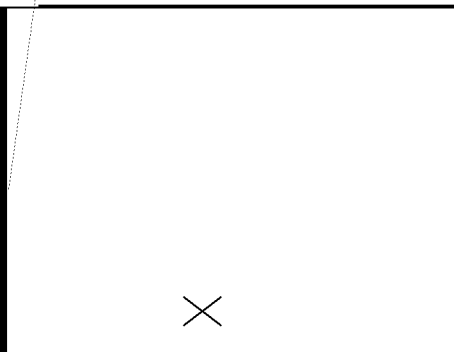
(S)



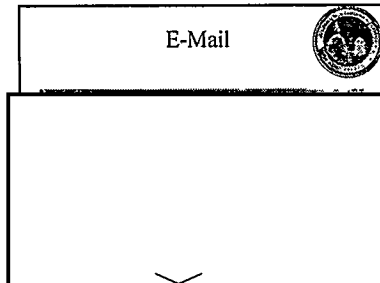
(S)



(S)

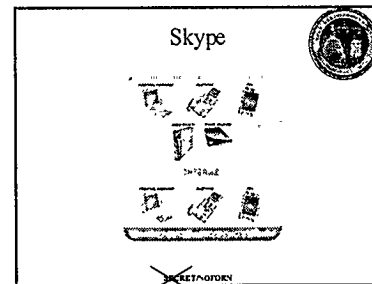
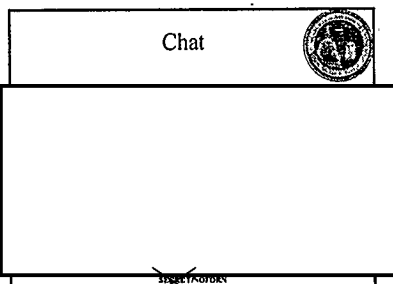
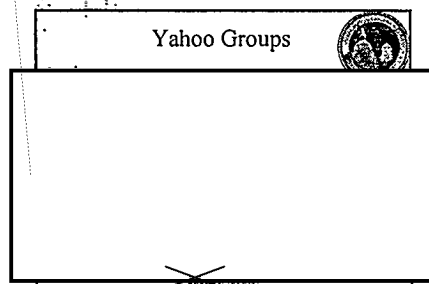


b1
b7E



b6
b7C
b7E

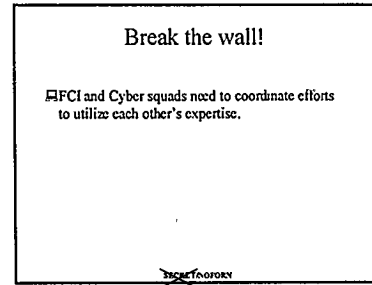
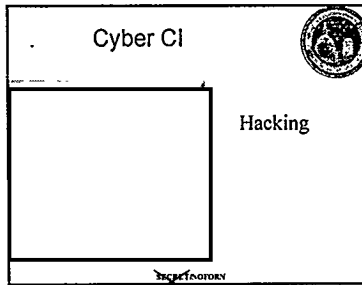
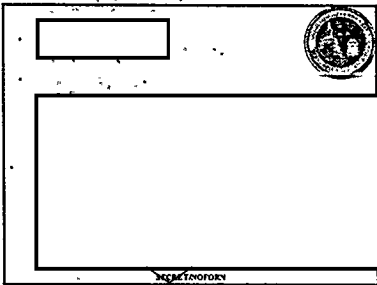
(S)



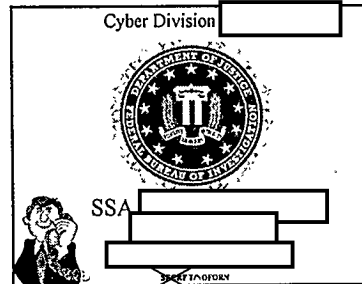
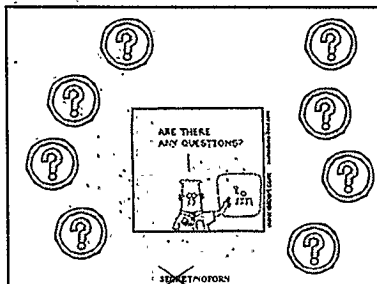
b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~



b7E



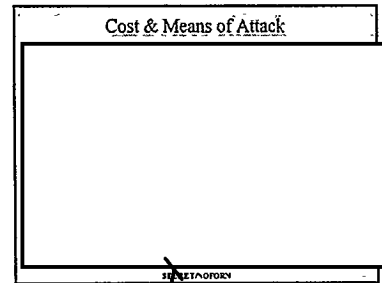
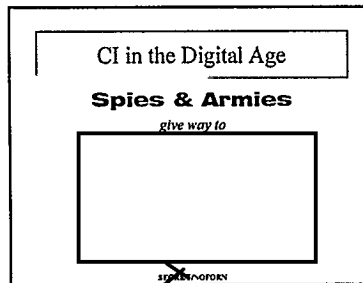
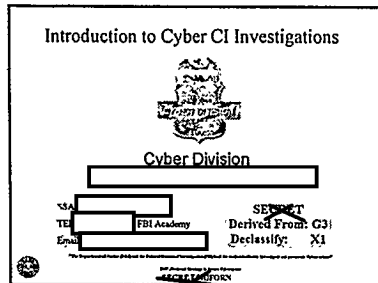
b6
b7C
b7E

~~SECRET~~

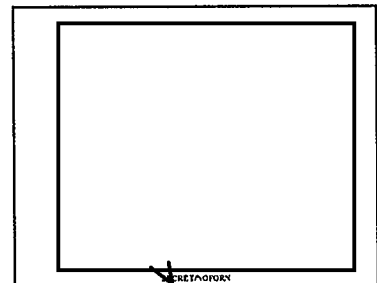
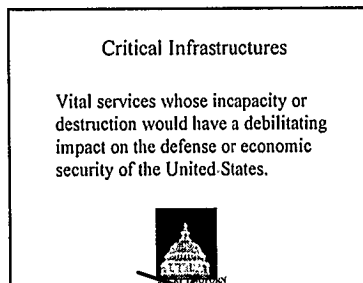
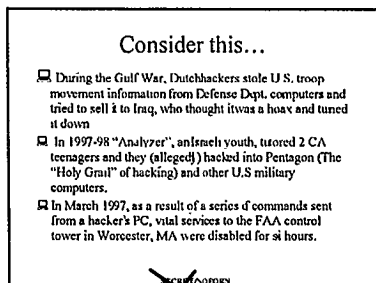
DATE: 02-08-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-08-2037

~~SECRET~~

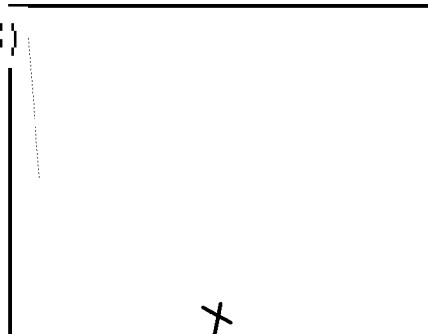
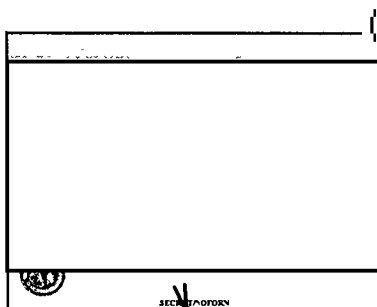
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b6
b7C
b7E



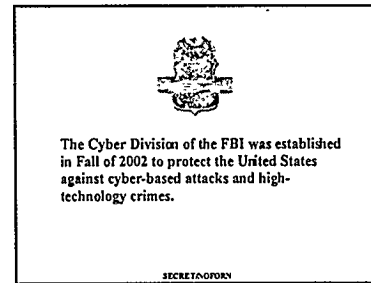
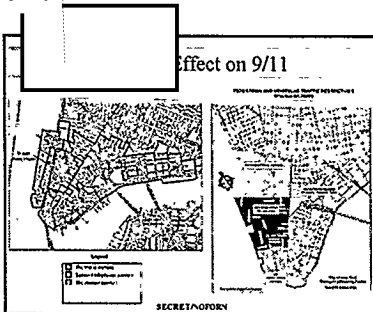
b7E



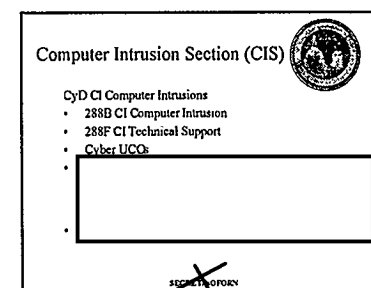
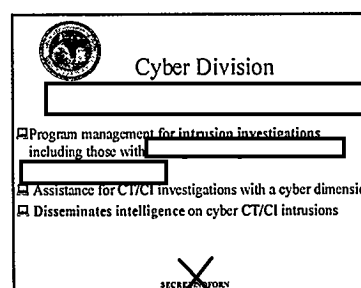
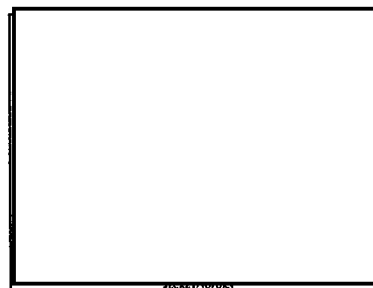
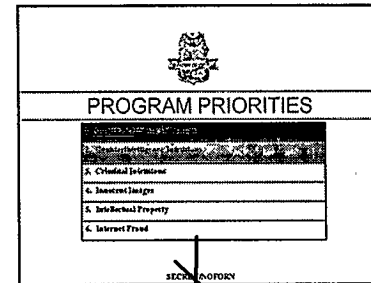
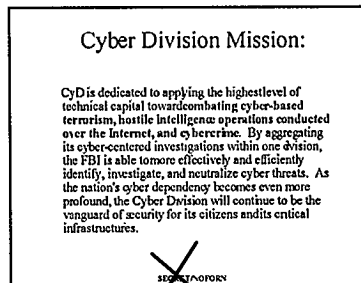
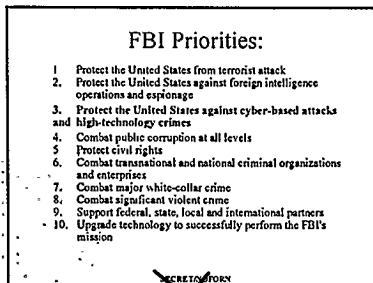
~~SECRET~~

~~SECRET~~

(S)



b1
b7E



b6
b7C
b7E

~~SECRET~~

~~SECRET~~

CT/CI Intrusion Cases
FY 2002 - 2006





~~SECRET//NOFORN~~

CI Intrusion Investigations



- Deconfliction/Coordination with CD in the field office and at FBIHQ substantive desks.
- Technical Support to CI Program
 - CI Investigation with cyber  requiring the expertise of a trained cyber agent:
 - Reading e-mail headers
 - Obtaining Internet Protocol (IP) information
 - Technical aspects of a UCO

~~SECRET//NOFORN~~

Why the Need for Deconfliction?



- Growing number of Cyber/CI investigations
- Prevent duplicative efforts
- Enhances communications/awareness
- Leads to coordinated efforts
- Identify best practices
- Mandated by 

~~SECRET//NOFORN~~

b7E

Counterintelligence Division

How Cyber's Mission relates to CI's Mission:

- > Prevent or neutralize the foreign acquisition of WMD or related equipment
- > Prevent penetration of Intel Community, USG, and sensitive contractor networks;
- > Prevent the compromise of the 
- > Conduct aggressive Cyber CI operations on most significant threat countries.

~~SECRET//NOFORN~~

(S)



CI National Intelligence Council/ National Intelligence Estimate Cyber Threats to the United States Information Security and Privacy (2004) 8

~~SECRET//NOFORN~~

(S)



CI National Intelligence Council/ National Intelligence Estimate Cyber Threats to the United States Information Security and Privacy (2004) 8

~~SECRET//NOFORN~~

b1
b7E

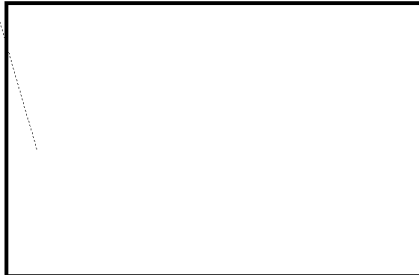
(S)



(S)



(S)



~~SECRET//NOFORN~~

~~SECRET~~

~~SECRET~~

(S)



☐ "China Operates the most extensive, technologically sophisticated and broad reaching system of internet filtering in the world"

☐ "The Chinese are successfully developing a market economy, at the same time they are continuing to accomplish control of the Internet"

☐ "Chinese censorship claim as many as 30,000 Internet Police"

Washington Post April 14, 2005

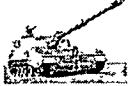
~~SECRET/NOFORN~~

☐ "India, China Hoping to Reshape the World Order Together"

☐ Pledge of New Strategic Alliance

☐ "If India and China Cooperate in the IT Industry, We Will Lead the World"

Chinese Premier Wen Jiabao



Washington Post April 14, 2005

~~SECRET/NOFORN~~



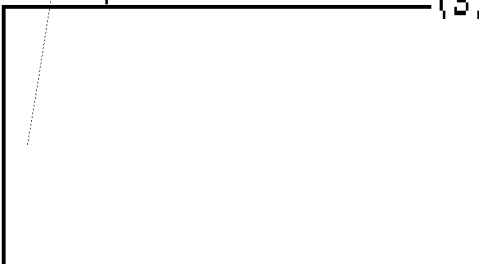
~~SECRET/NOFORN~~

b1
b7E

(S)

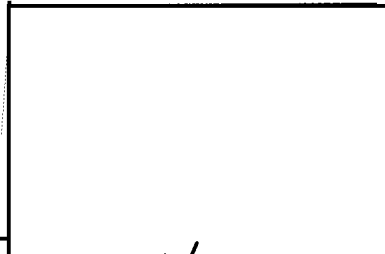
(S)

(S)



For National Intelligence Council Internal Information Use Only: Cyber Threats to National and Global Information Infrastructure February 2004

~~SECRET/NOFORN~~



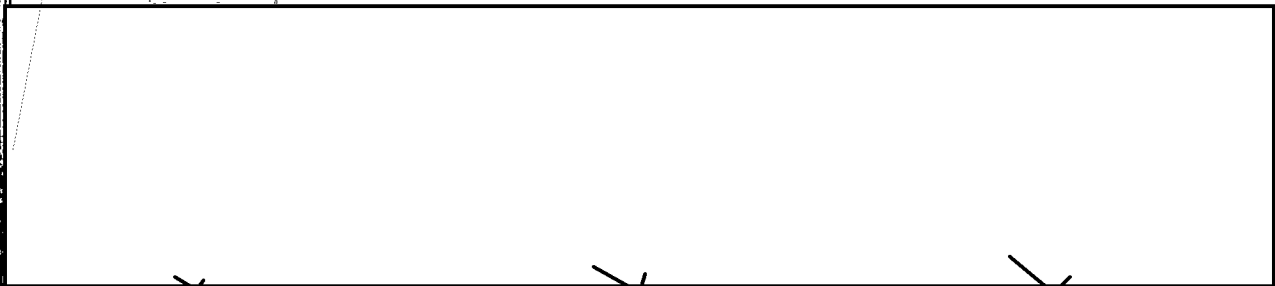
~~SECRET/NOFORN~~



~~SECRET/NOFORN~~

b1
b7E

(S)



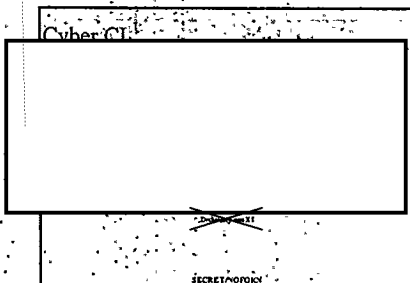
~~SECRET/NOFORN~~

b1
b7E

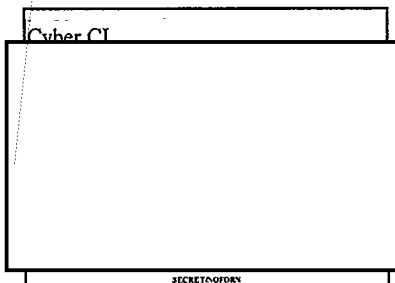
~~SECRET~~

~~SECRET~~

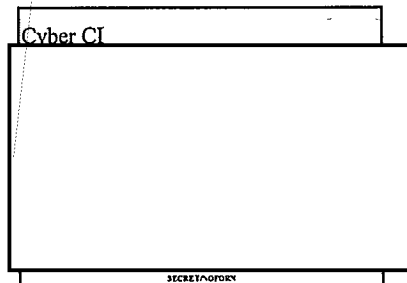
(S)



(S)

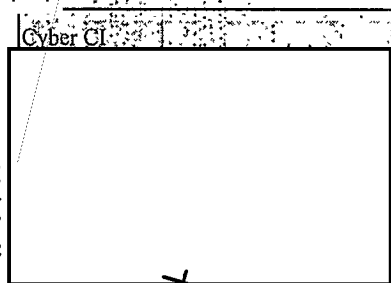


(S)

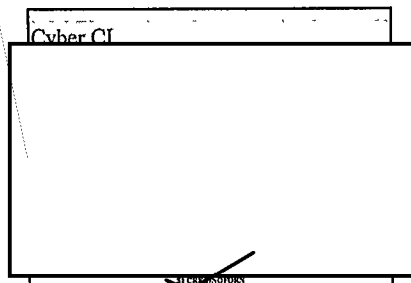


b1
b7E

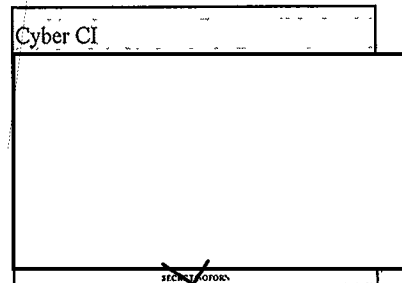
(S)



(S)

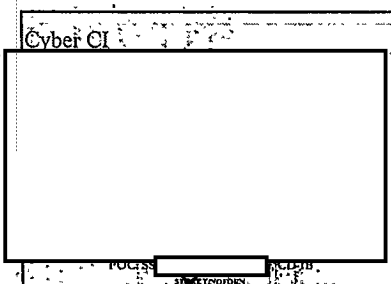


(S)

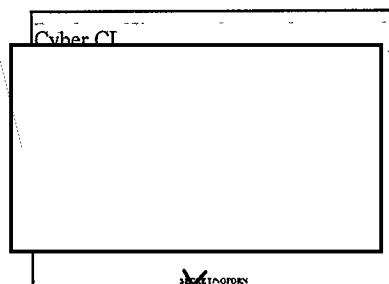


b1
b7E

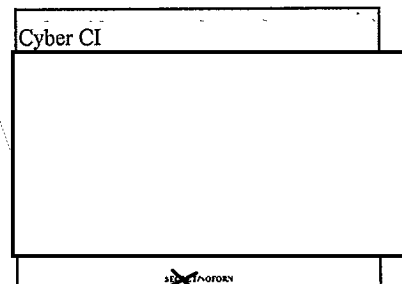
(S)



(S)



(S)



b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

(S)

Cyber CI Cyber CI Cyber CI

[Redacted]

b1
b7E

~~SECRET//NOFORN~~ ~~SECRET//NOFORN~~ ~~SECRET//NOFORN~~

(S)

Cyber CI Cyber CI

[Redacted]

[Redacted]
• Trained at KGB Higher School
• Expert in cryptology
• Worked at [Redacted]
• May exaggerates cyber threats to benefit his business [Redacted]

b1
b6
b7C
b7E

~~SECRET//NOFORN~~ ~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

Cyber CI Cyber CI Cyber CI

[Redacted]

b1
b7E

~~SECRET//NOFORN~~ ~~SECRET//NOFORN~~ ~~SECRET//NOFORN~~

~~SECRET~~

(S)

Cyber CI

[Redacted]

- How does the US government detect viruses on their computers?
- Can the US govt. tell if a hacker broke into other systems?
- Can the US govt. track an IP address overseas?

~~SECRET~~

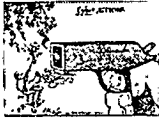
(S)

Cyber CI

Trends & Emerging Threats

- Targeting of infrastructure
- Thinking enemy with independent will
- Compromise of Sensitive Bot
- Unlawful (SBU) Networks
- Use of improved bandwidth to facilitate criminal activity
- Increased social engineering
- Non-malevolent Trojans
- "Preparing the Battlefield"

Spies screen



~~SECRET~~

Cyber CI

Tools [Redacted]

Who needs dual drops and brush passes these days?

- Internet
- E-mail
- VoIP
- ICQ
- IM
- Chat Rooms

[Redacted]

~~SECRET~~

b1
b7E

(S)



b1
b7E

(S)



~~SECRET~~

(S)

Cyber CI
Tools & [redacted]

Intelligence Operative Use of the Internet

- Facilitate
- C³
- Command
- Control
- Communications

[redacted]

- Identification of UCE's
- Target Reconnaissance

~~SECRET/NOFORN~~



Cyber CI
Tools & Websites

[redacted]

~~SECRET/NOFORN~~

b1
b7E

(S)

Cyber CI
Tools & [redacted] E-mail

[redacted]

~~SECRET/NOFORN~~

Cyber CI
Tools & [redacted] Online Communities

[redacted]

~~SECRET/NOFORN~~

Cyber CI
Tools & [redacted] Chat

[redacted]

~~SECRET/NOFORN~~

b1
b7E

Cyber CI
Tools & [redacted] Voice Over IP

[redacted]

~~SECRET/NOFORN~~

Cyber CI
[redacted]

CI and Cyber squads need to coordinate efforts and utilize each other's expertise.

[redacted]

~~SECRET/NOFORN~~

[redacted]


Questions

~~SECRET/NOFORN~~

b7E

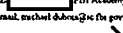
~~SECRET~~

~~SECRET~~

Introduction to Cyber CI Investigations



Cyber Division

SS  ~~SECRET~~
TE  FBI Attorney Derived from: G3
Email: michael.dubois@ic.fbi.gov Declassify: X1

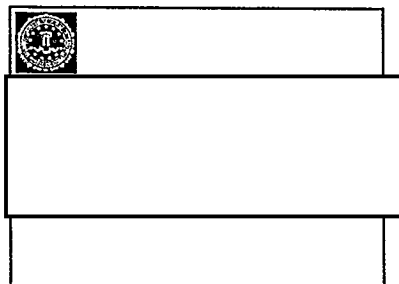
~~SECRET NOFORN~~

b6
b7C
b7E

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



Technical Operations

■ The most useless thing is something done at great cost that need not have been done at all.

Technical Operations

Are:

- Costly\$\$\$\$\$\$
- Manpower Intensive
- before, during & after

b7E

(S) Where Did We Get This Stuff?

- FBI - school of hard knocks
- Military
- Business - Project Management/PMI

■ The principles are common.

First Thing

■ The first thing is not:

■ The first thing is "Define the Requirements".

Why Requirements?

b1
b7E

Defining Requirements

First POC at Field is

They should:

Requirements on Significant Attacks

Write these down and communicate them.

Requirements

A Typical Scenario:

1. No such thing - each technical attack is unique
 - Quick Reaction
 - Time on Target
 - Long Term Objectives
 - Desired Realistic Results
 - Construction vs. Trojan
 - Hard Target vs. Soft Target
 - Cost to Benefit Analysis

b7E

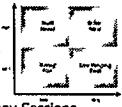
~~SECRET~~

Requirements

A Typical Scenario:

- Laying out Requirements – Targeting and Prioritizing

- Survey Strategies
- Talking Over Options
- Include Techs In Strategy Sessions



10

Requirements

A Typical Scenario:

- Communication with HQ




11

Requirements

A Typical Scenario:

- Operations Planning

- Responsibilities
- Duties
- Op Order / S paragraph order (SMEAC)
- Lessons Learned



12

b7E

Requirements

A Typical Scenario:

- Post Operations Follow-Up

- Continued Support
- Language Services
- Long Term vs. Short Term



13

Other Considerations

Legal

Technical

- tech request
- time
- realistic approach

Overseas Operations

OGA/USIC Technical Cooperation



14

Other Considerations

OGA/USIC Technical Cooperation

- R&D Projects
- Case Examples
 - Working It the Right Way
 - Working It the Wrong Way
- Controlling Expectations
 - The "Enemy of the State" Syndrome



15

Requirements

- #1 Sin: Starting with the solution predefined for complex tech ops.
 - There is no canned solution – (does not apply to gimme's)
- #2 Sin: Failure to Prioritize and Target.
- #3 Sin: Failure to Communicate.

16

Risk Assessment



17

Communicate Risk

- Need a basis for common understanding.
- In 1951 a NI E stated the invasion of Yugoslavia by the Soviet Union was a "serious possibility".
- The w nter estimated this to mean 65 to 35 in favor of invasion.
- The ch airman of the DS Planning Staff estimated much lower odds.
- Esti mates varied between 20 to 80 and 80 to 20.

18

b6
b7C
b7E

~~SECRET~~

Risk Assessment





19

Communicate Risk

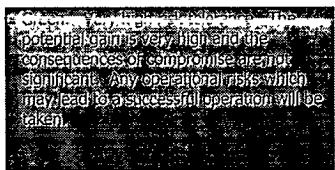


Red - Very low risk tolerance. A risk of compromise resulting from a cost of 100 is unacceptable. Compromise of the operation has severe consequences, particularly when weighed against the potential gain. The intelligence gain in this case would be vastly outweighed by the costs of discovery and disclosure. The operations will be aborted at the slightest problem. Operational objectives will be sacrificed for operational security.

20

Communicate Risk



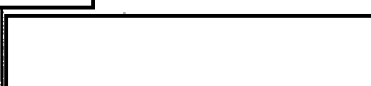


21

b7E

Risk Assessment





22

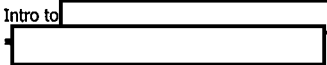


Discussion

23

Risk Assessment



Intro to 



24

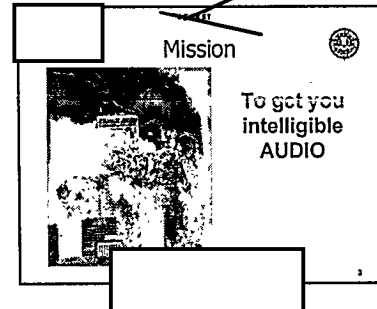
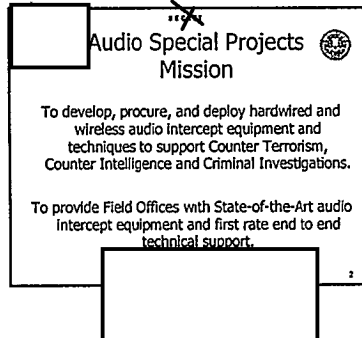
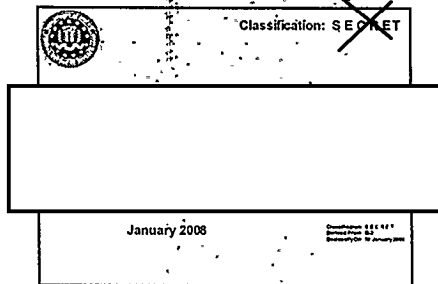
b7E

~~SECRET~~

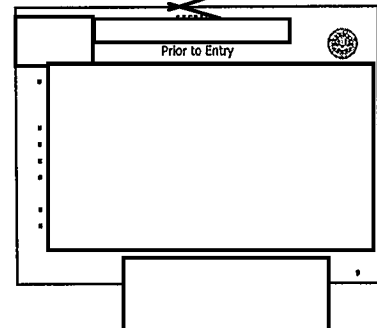
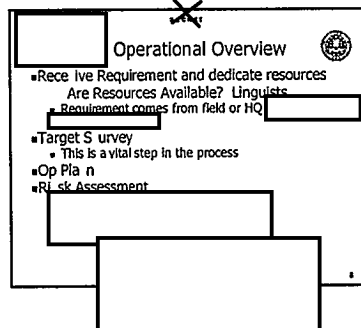
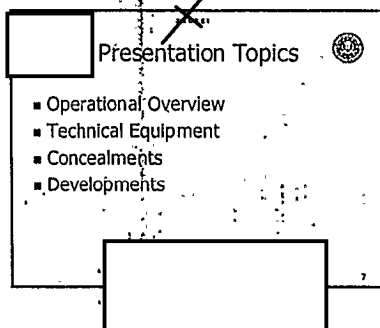
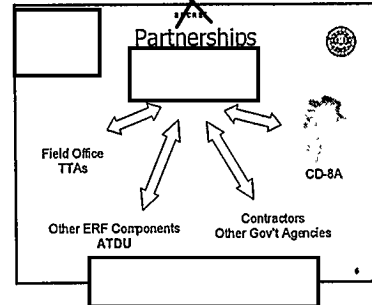
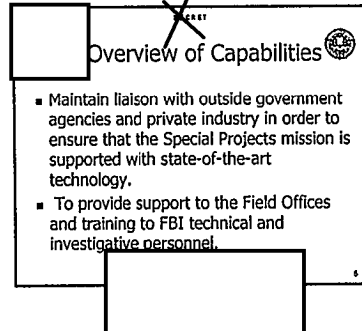
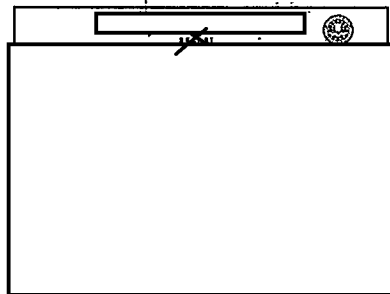
DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



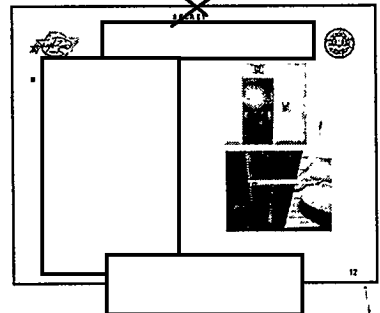
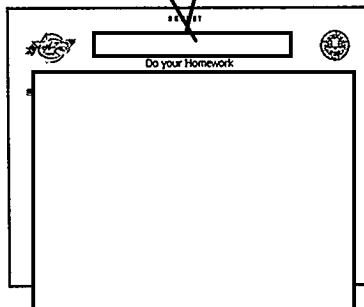
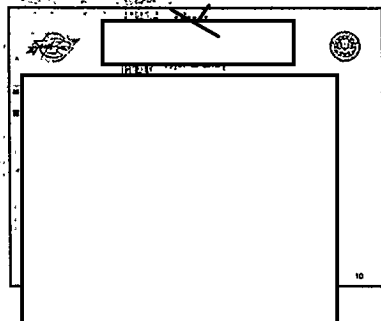
b7E



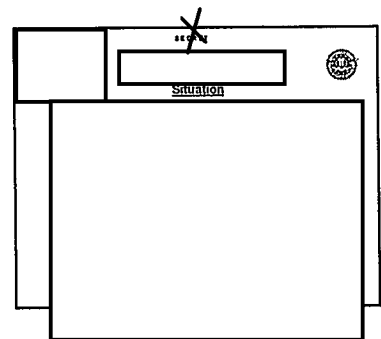
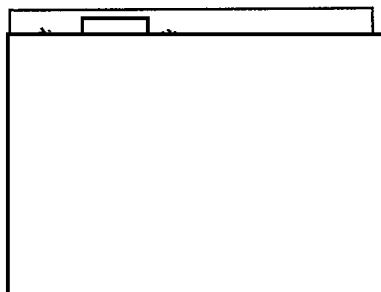
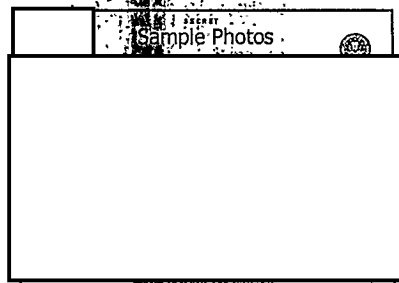
b7E

~~SECRET~~

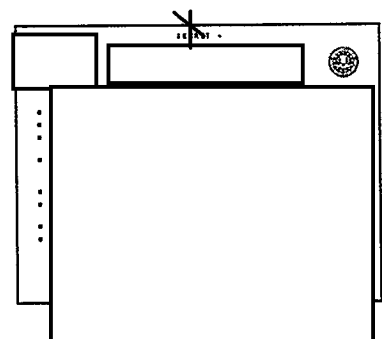
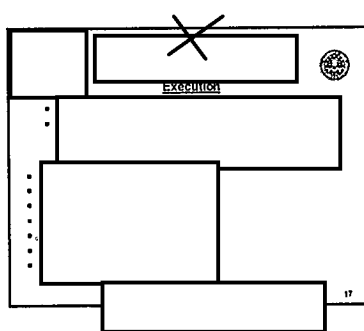
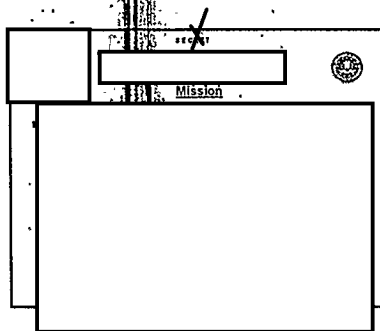
~~SECRET~~



b7E



b7E



b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

Execution

- Court Order—establish the legal authority and authorized actions.
- Debrief: If there is to be one where, when and who should attend.

[Redacted]

19

~~SECRET~~

Service and Support

[Redacted]

20

~~SECRET~~

Command and Communications

[Redacted]

21

b1
b7E

(S)

~~SECRET~~

[Redacted]

- Unclassified time line.
- Contact information.

[Redacted]

22

~~SECRET~~

Identify Appropriate Equipment

[Redacted]

23

~~SECRET~~

Basic Strategy

[Redacted]

(S)

(S)

b1
b7E

~~SECRET~~

Basic Technology

... then look at the technologies necessary to do the collection.

[Redacted]

24

~~SECRET~~

[Redacted]

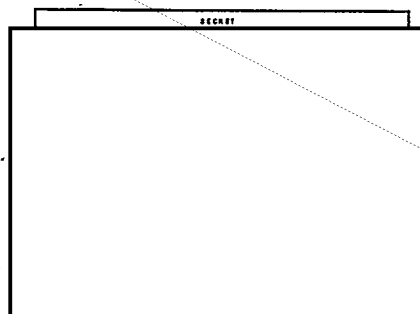
~~SECRET~~

[Redacted]

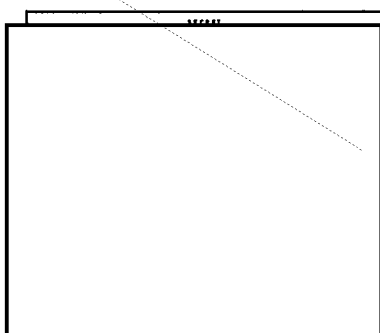
~~SECRET~~

~~SECRET~~

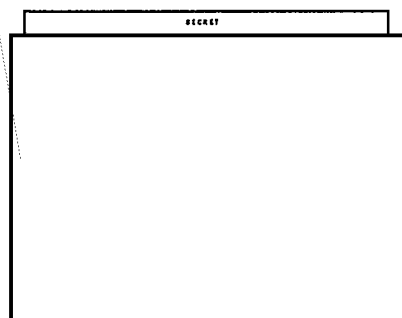
(S)



(S)



(S)



b1
b7E

~~SECRET~~

**Technologies
Microphones**

- Standard Air Path
- Optical
- Contact



31

~~SECRET~~

**Technologies
Hardwire**

**THE BEST TYPE OF ATTACK
Unlimited Lifespan**

- Hardwire
- Telephone
- Cable
- Fiber
- Power line



32

~~SECRET~~

**Technologies
Radio Frequency (RF)**

- Designed for low power
- High reliability
- Require a Listening Post in close proximity
- Typically present a higher TSCM profile
- Store and forward applications

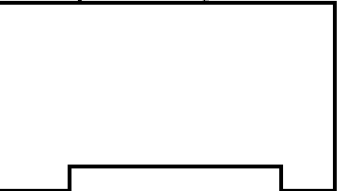


33

b1
b7E

~~SECRET~~

Technologies



34

~~SECRET~~

Technologies



35

(S)

~~SECRET~~

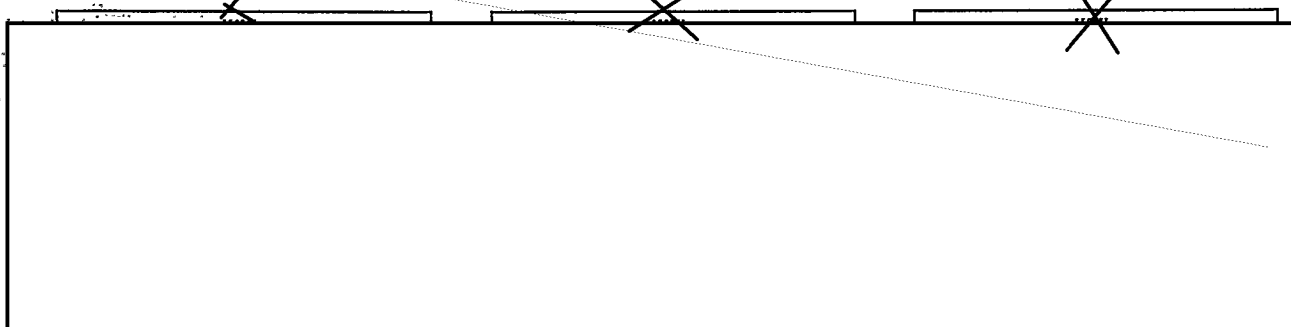


36

~~SECRET~~

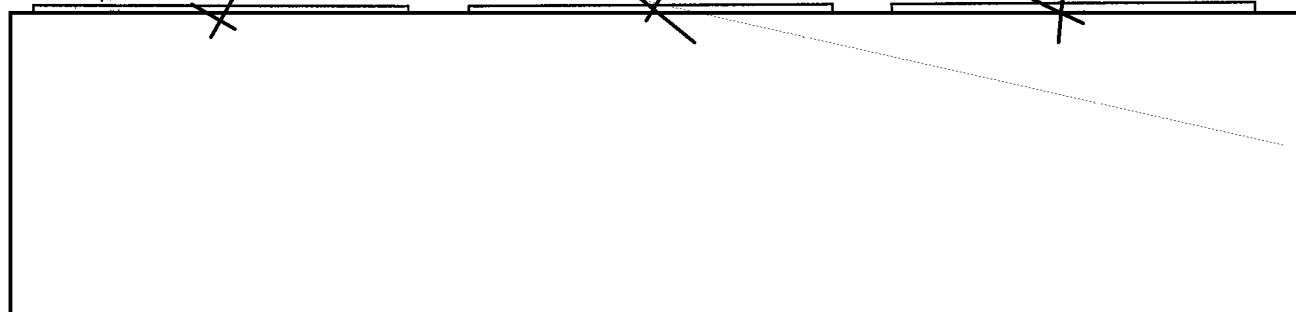
~~SECRET~~

(S)

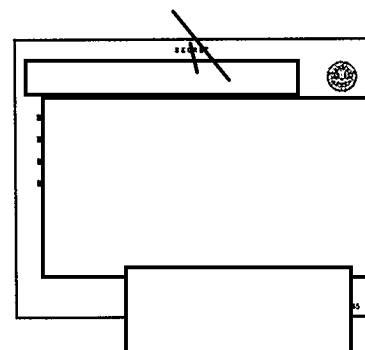
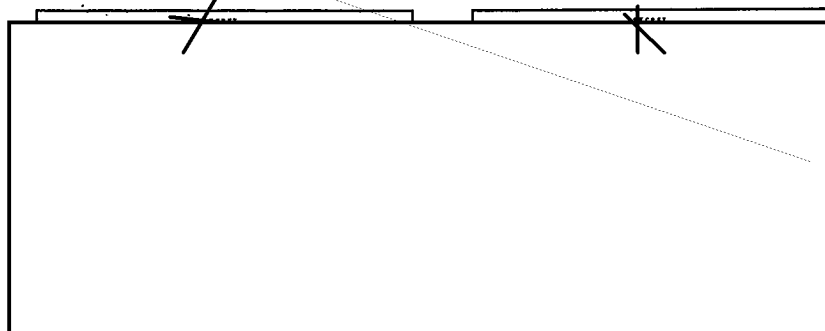


b1
b7E

(S)



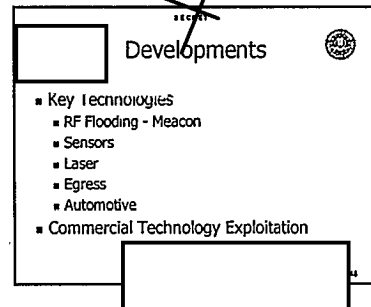
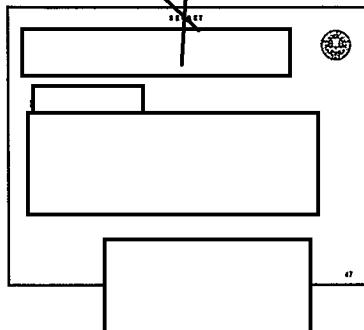
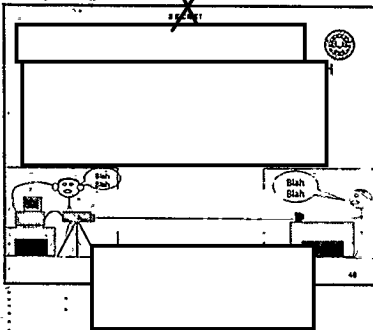
(S)



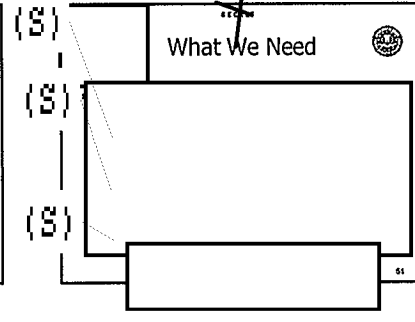
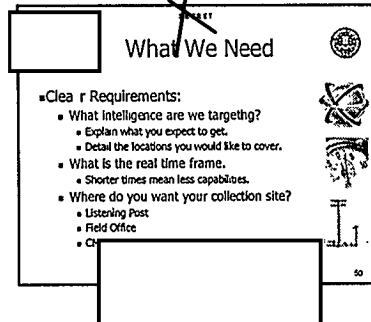
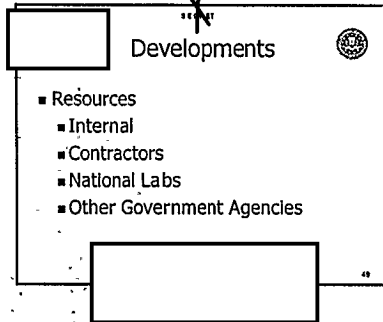
b1
b7E

~~SECRET~~

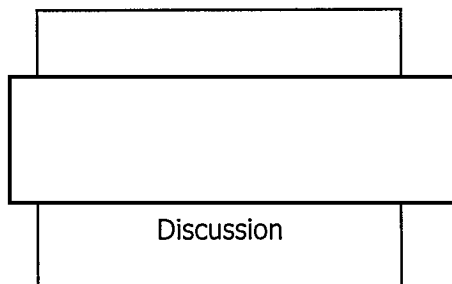
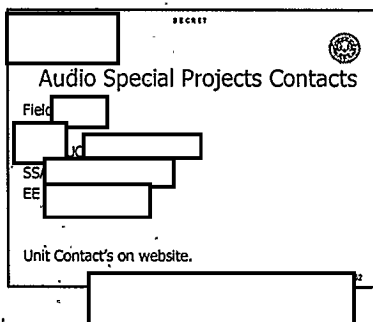
~~SECRET~~



b1
b7E



b6
b7C
b7E

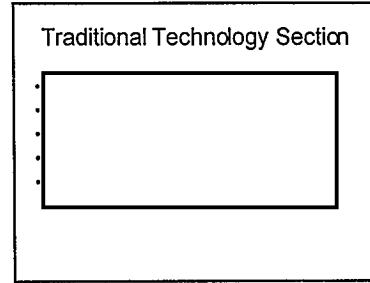
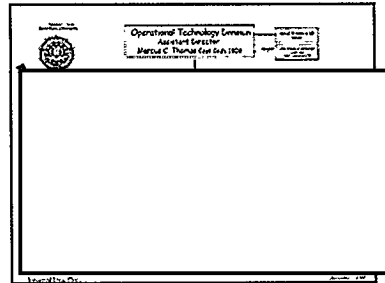
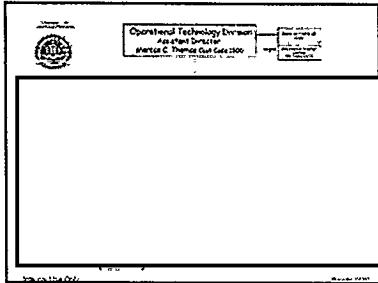


~~SECRET~~

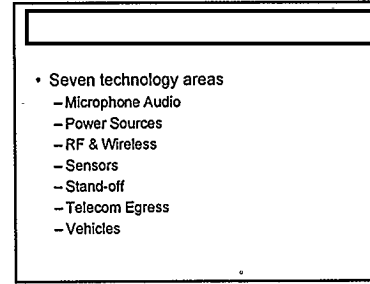
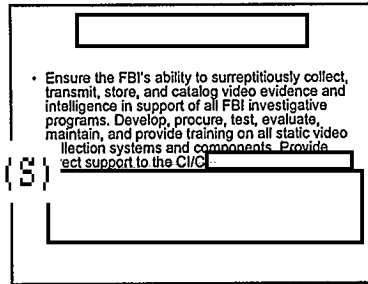
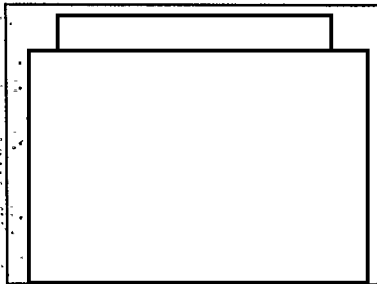
DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

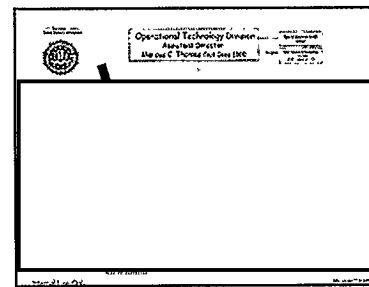
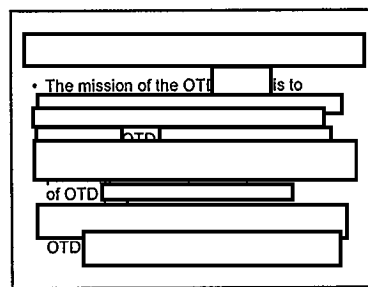
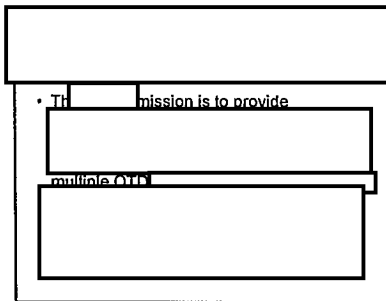
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b7E



b1
b7E



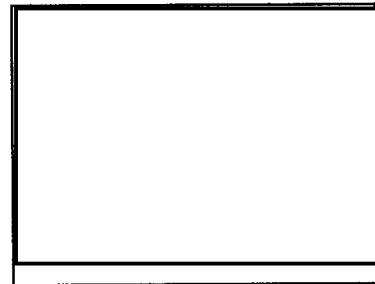
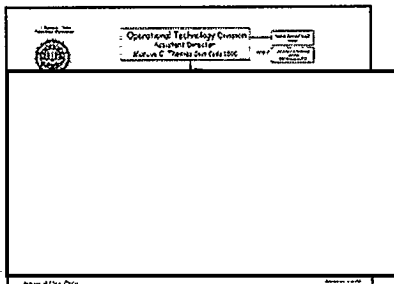
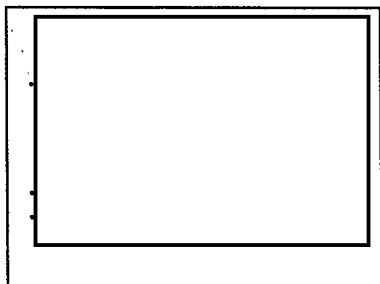
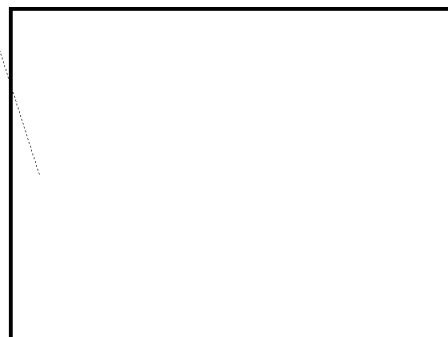
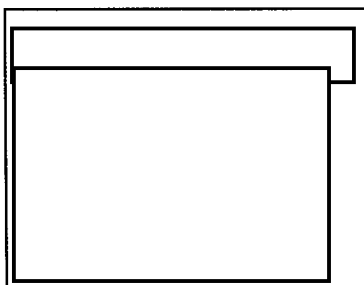
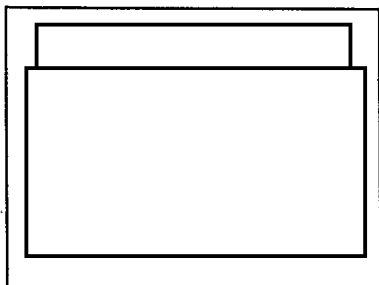
b7E

~~SECRET~~

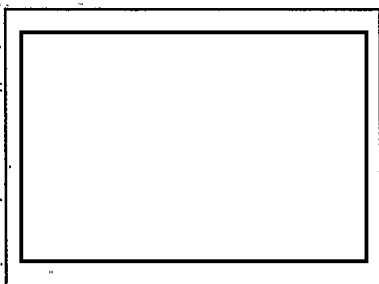
~~SECRET~~

(S)

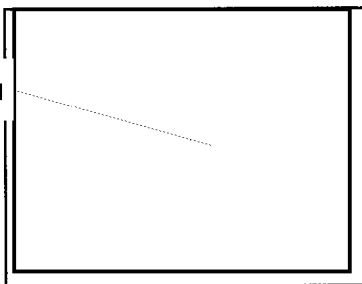
b1
b7E



b7E



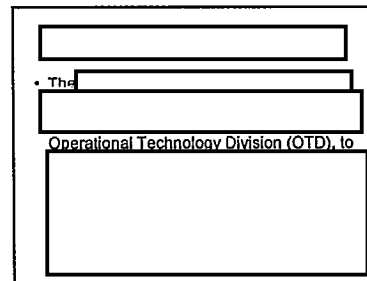
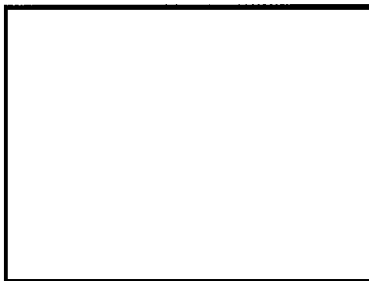
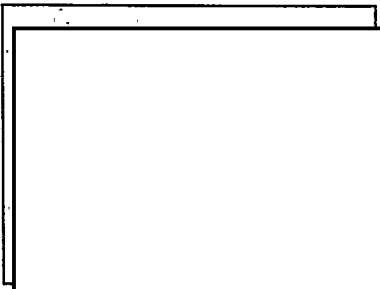
(S)



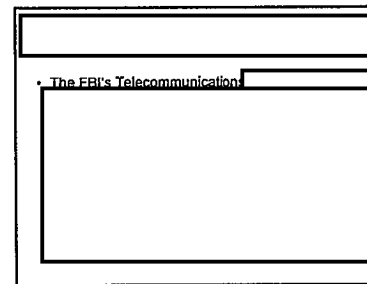
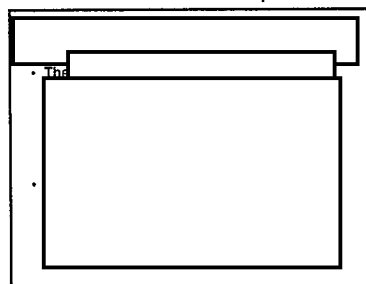
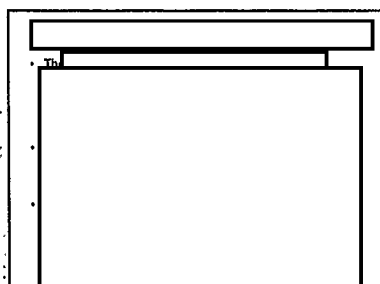
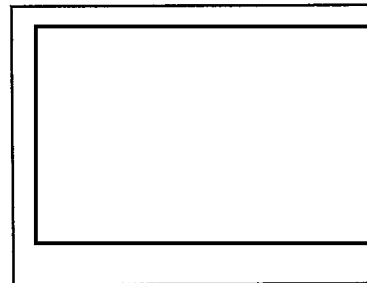
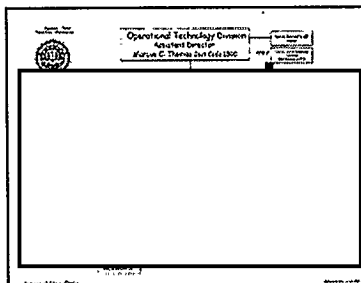
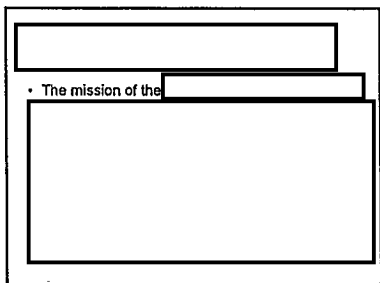
b1
b7E

~~SECRET~~

~~SECRET~~



b7E



b7E

~~SECRET~~

~~SECRET~~

(S)

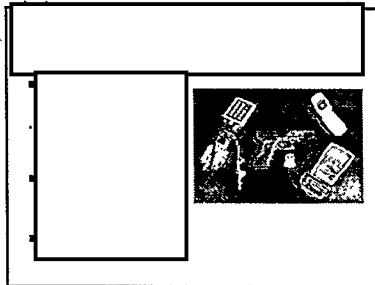
- The

b7E

FBI041893

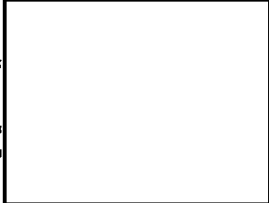
~~SECRET~~

DECLASSIFIED BY 65179 DMH/STW
ON 02-15-2012



Regional Coordination Group

- U.S. divided into six regions
- Supports technical operations
- Selects new candidates



- Interview

b7E

Basic Classes

- Basic Electronics (80 classroom hours)
- Basic Video (80 classroom hours)
- Basic Microphone/Audio (40 classroom hours)
- Basic Telephony (40 classroom hours)
- Computers for TTAs (40 classroom hours)
- Tracking (40 classroom hours)

Basic Electronics

- SAFETY1
- Electric theory
- Basic formulas
- AC and DC wiring
- Transformers
- Regulators
- How to assemble components into systems



Basic Video

- Cameras
- Optics and lenses
- Night vision/thermal imaging
- Concealments
- Video transmission systems
 - Hardware
 - Microwave
 - Video over IP



Basic Microphone / Audio

- Audio theory
- Microphone types
- Microphone placement
- Microphone concealment
- Audio egress systems



Basic Telephony

- The telephone system
- Intercept
- Voice collection
- Data collection



Computers for

- Computer components
- Computer systems
- Computer networks

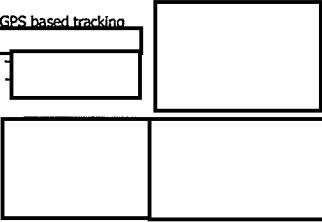


b7E

~~SECRET~~

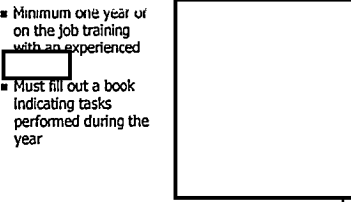
Basic tracking

- GPS based tracking



On the job training

- Minimum one year of on the job training with an experienced
- Must fill out a book indicating tasks performed during the year



Certification

- Eligible for Certification after:
 - Spending at least one year in on-the-job training
 - Completion of book of tasks
 - Successful completion of practical exercises

b7E

Practical Exercises

- Scenario based problems
- Students work in pairs
- Examples



Advanced training continuing education

- Audio and video installation techniques
- Land navigation
- Advanced tracking systems
- Covert entry
- And many more...



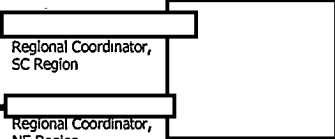
Professional organizations

- National Technical Investigator's Association (NATIA)
 - Membership in NATIA
 - At NATIA conventions, many vendors and equipment suppliers available...

b7E

Questions?

- Regional Coordinator, SC Region
- Regional Coordinator, NE Region



b6
b7C
b7E

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)





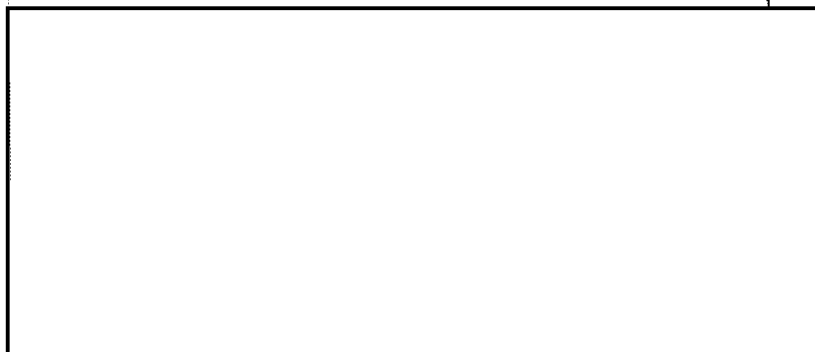
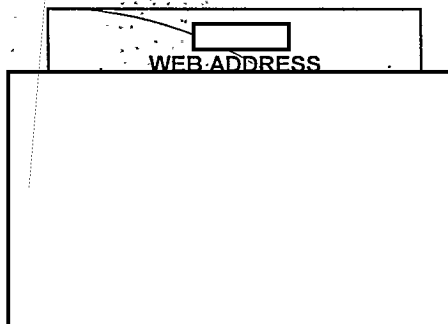
Getting Started

- As soon as you believe your case is moving in the direction of a surreptitious entry you need to advise your Technical Squad.
- The Tech Agent will immediately request our assistance with an EC

b1
b7E

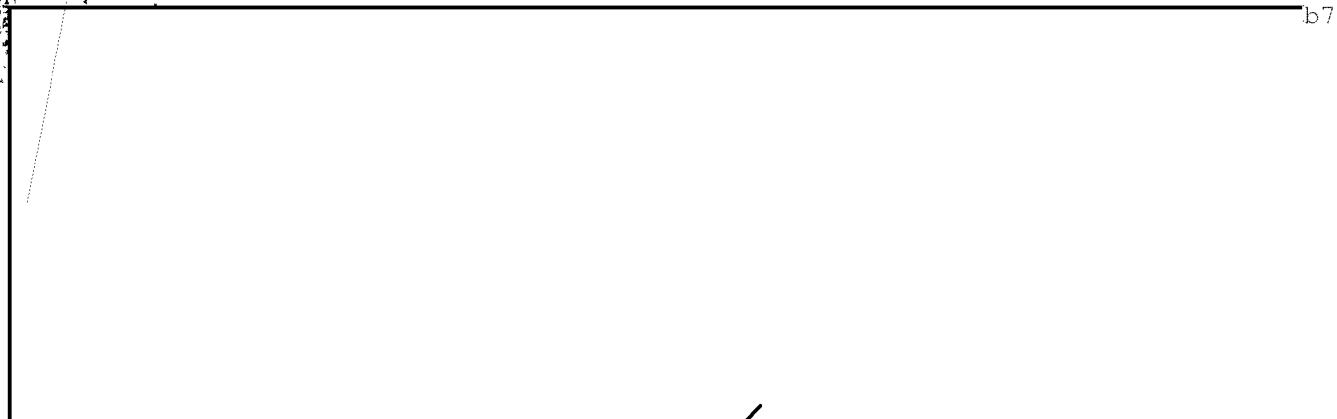
(S)

(S)



b1
b7E

(S)



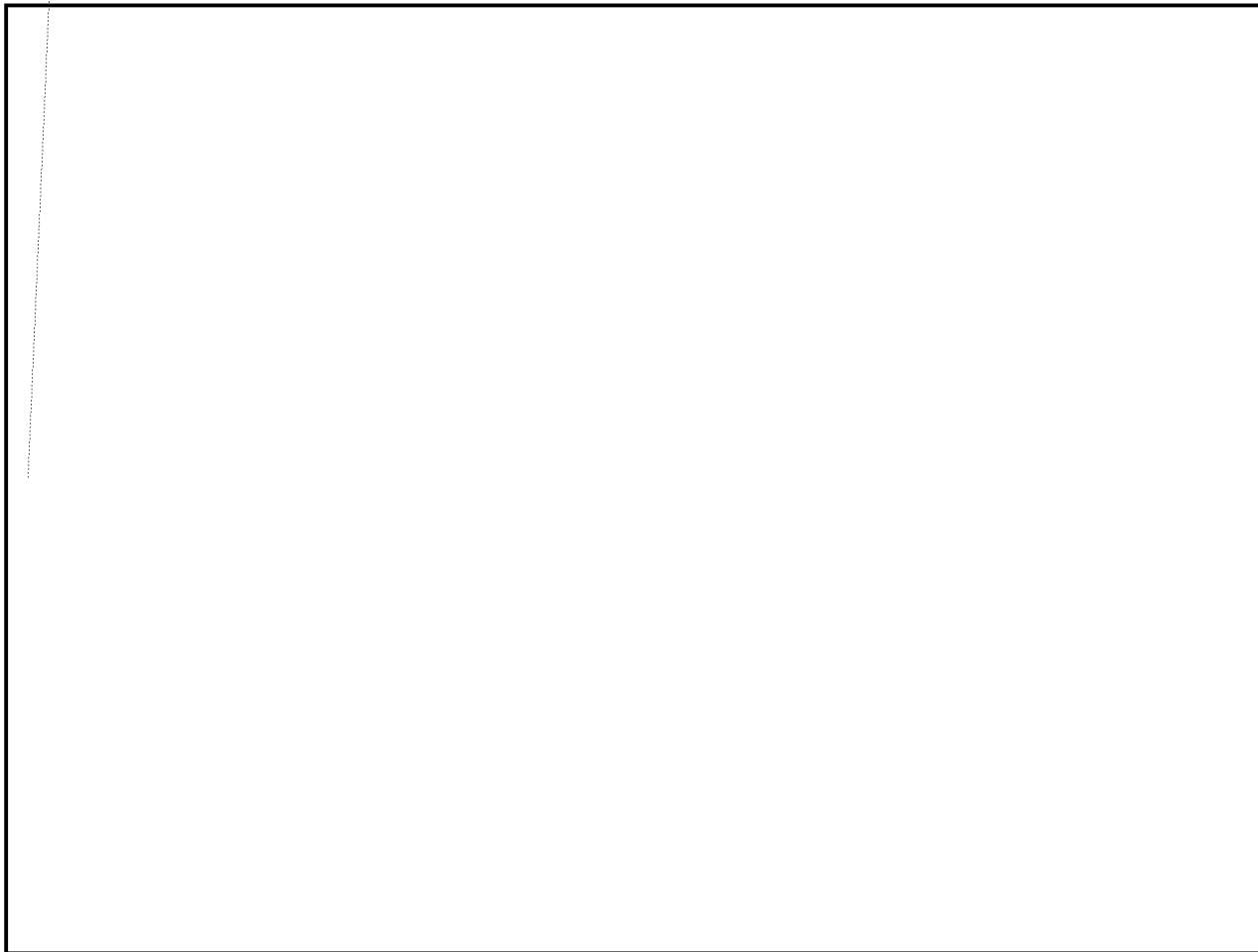
b1
b7E

~~SECRET~~

ACLURM042996

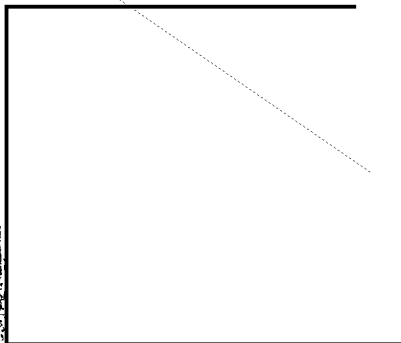
~~SECRET~~

(S)



b1
b7E

(S)



(S)



b1
b7E

Thank you!

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

OPERATIONAL TECHNOLOGY DIVISION
Tactical Operations Section

(S)

7/15/2011

(S)

Tactical Operations Support Center
(TOSC)

- A National Level Center
- Supporting FBI, intelligence and law enforcement communities

7/15/2011

(S)

TOSC

7/15/2011

b1
b7E

(S)

TOSC Organization

7/15/2011

(S)

TOSC Services

7/15/2011

(S)

7/15/2011

b1
b7E

(S)

7/15/2011

(S)

Mission

What we do

☐ Assist in Covert Entries

7/15/2011

(S)

7/15/2011

b1
b7E

~~SECRET~~

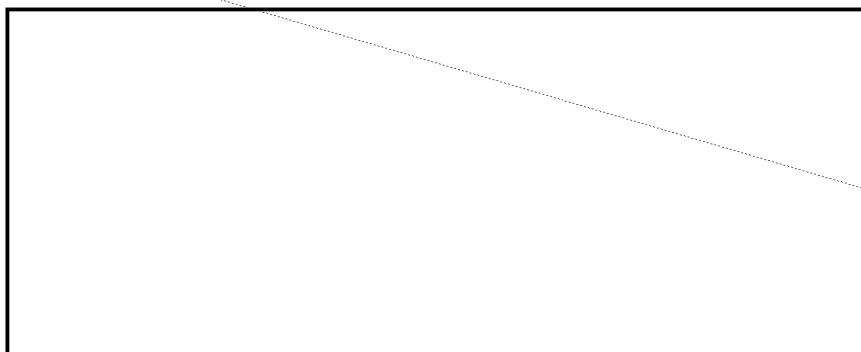
~~SECRET~~

(S)

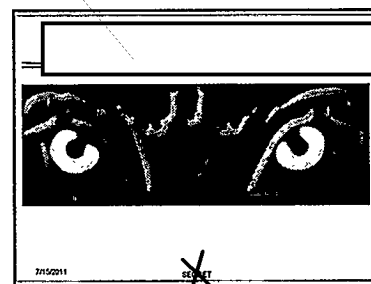


b1
b7E

(S)



(S)



b1
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02

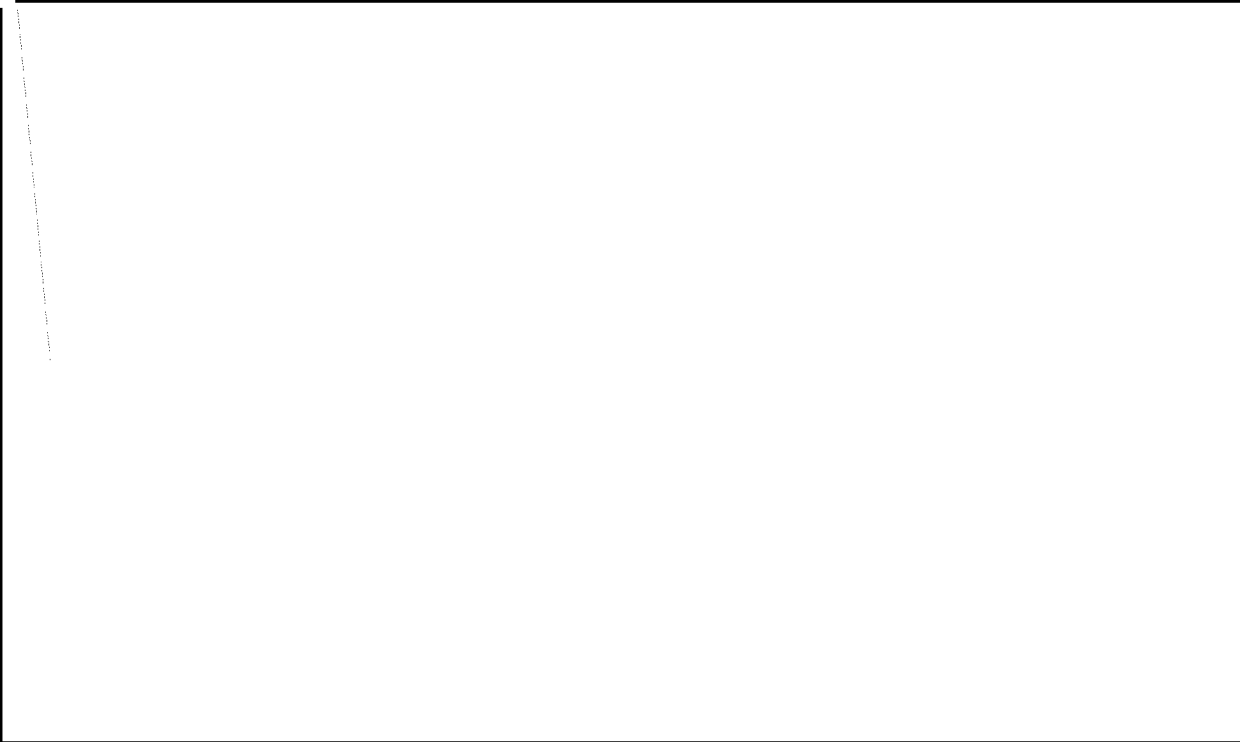
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



ENTRIES

(S)



~~SECRET~~

~~SECRET~~

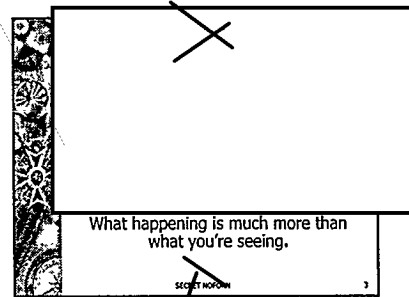
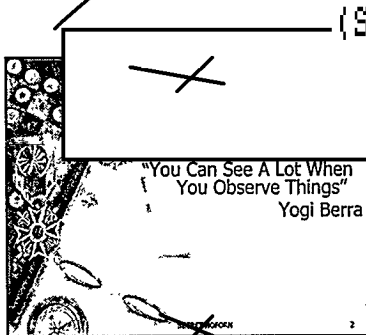
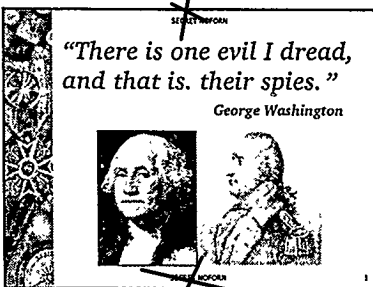
b1
b7E

~~SECRET NOFORN~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

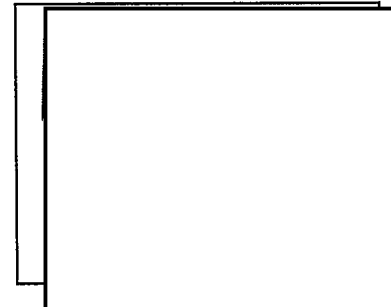
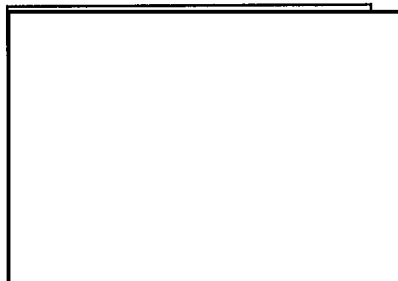
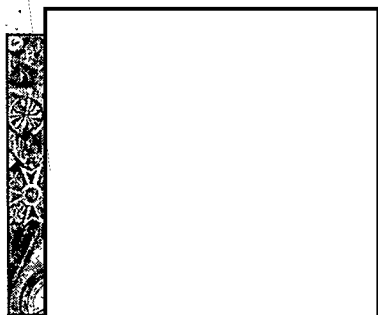
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



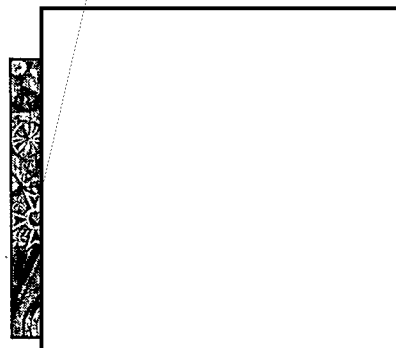
b1
b7E

(S)

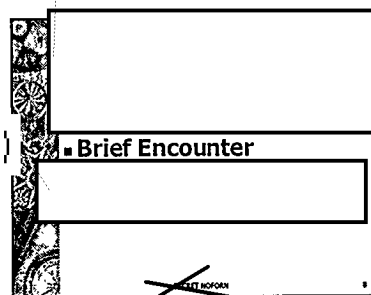


b1
b7E

(S)



(S)



(S)



b1
b7E

~~SECRET~~

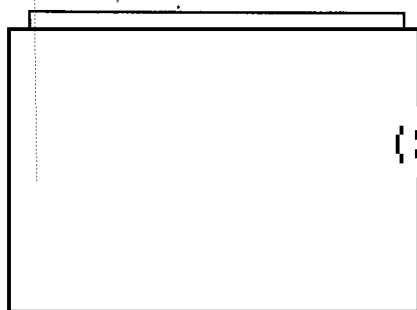
~~SECRET NOFORN~~

ACLURM043001

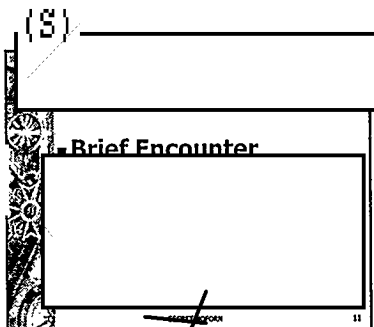
~~SECRET~~

~~SECRET NOFORN~~

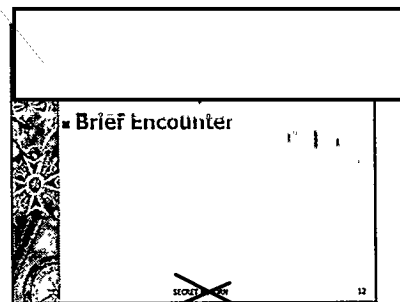
(S)



(S)

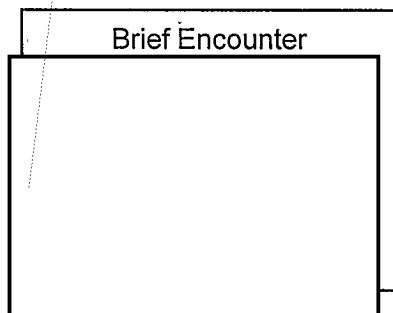


(S)



b1
b6
b7C
b7E

(S)

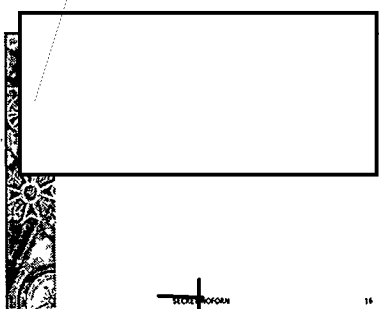


(S)

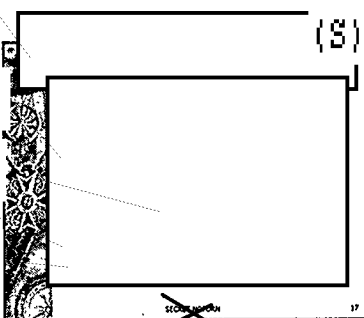


b1
b6
b7C
b7E

(S)

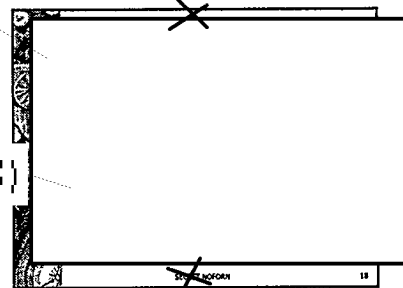


(S)



(S)

(S)



b1
b7E

~~SECRET~~

~~SECRET NOFORN~~

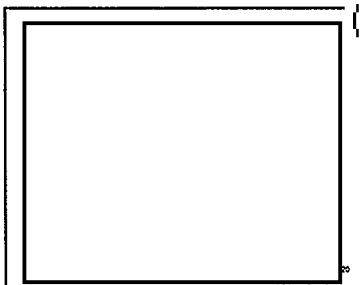
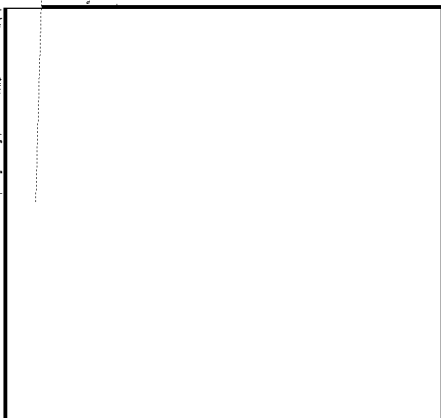
ACLURM043002

~~SECRET~~

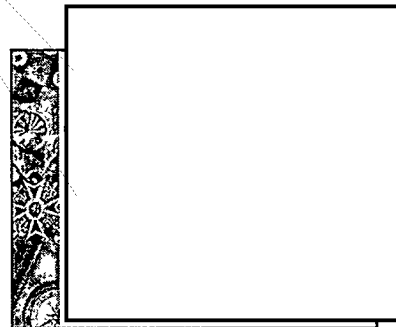
~~SECRET NOFORN~~

(S)

(S)

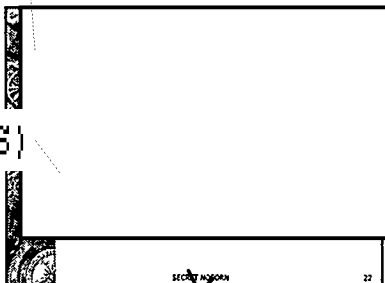


(S)

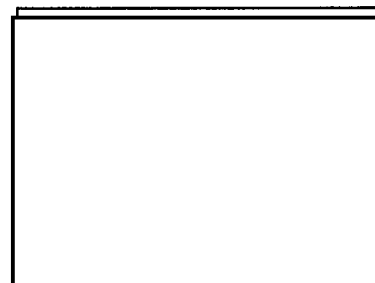
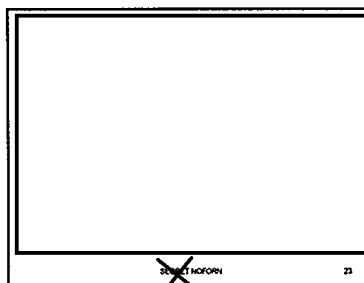


b1
b7E

(S)

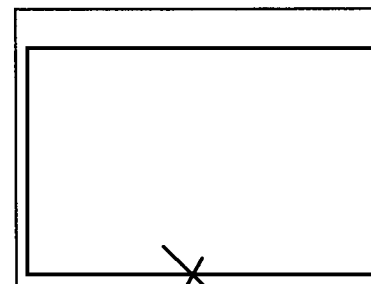
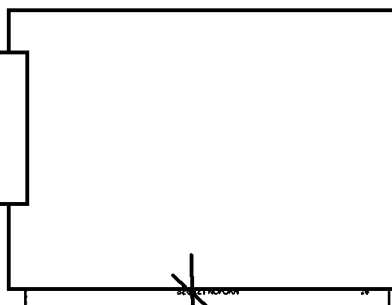
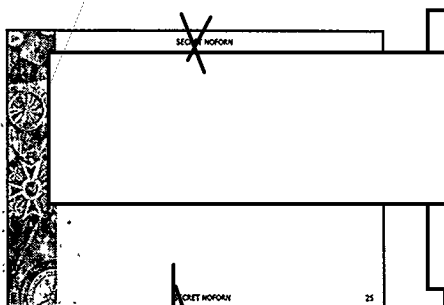


(S)



b1
b7E

(S)



b1
b7E

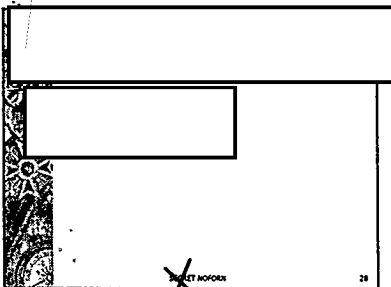
~~SECRET~~

~~SECRET NOFORN~~

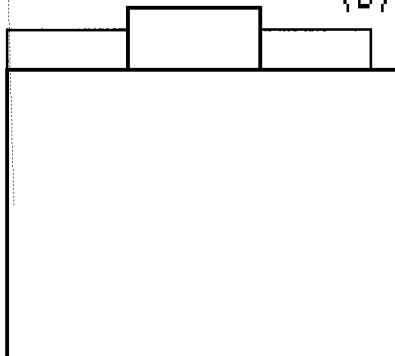
~~SECRET~~

~~SECRET NOFORN~~

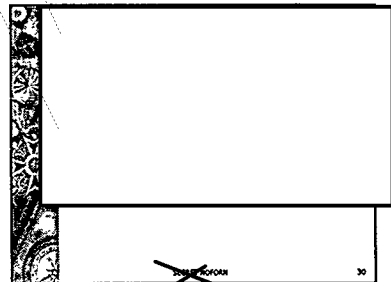
(S)



(S)

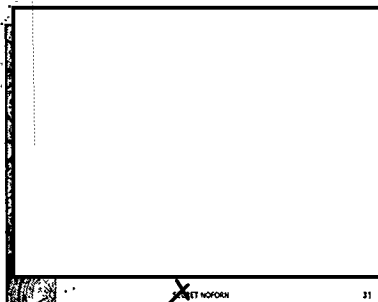


(S)

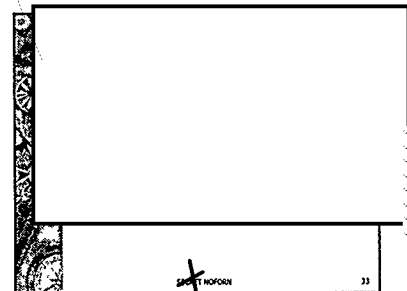
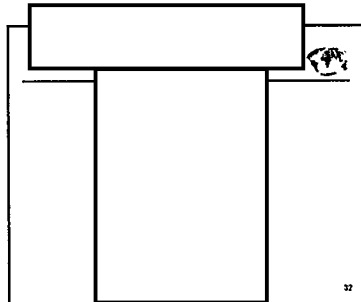


b1
b7E

(S)

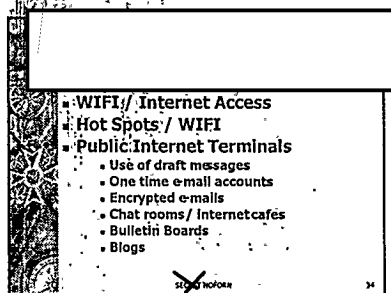


(S)

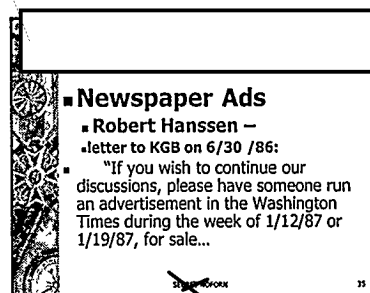


b1
b6
b7C
b7E

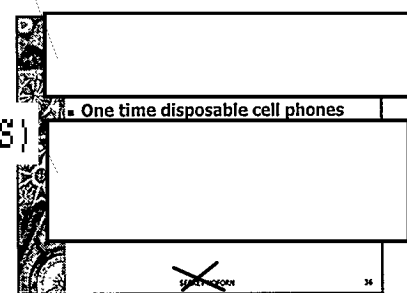
(S)



(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET NOFORN~~

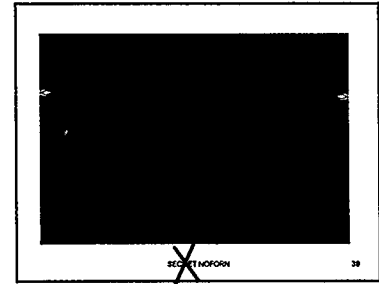
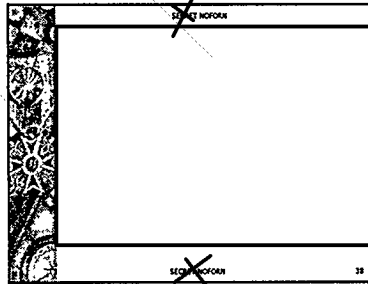
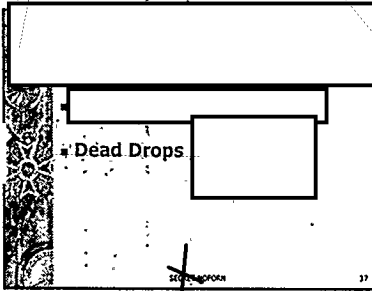
~~SECRET~~

~~SECRET NOFORN~~

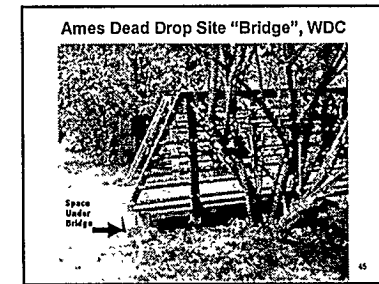
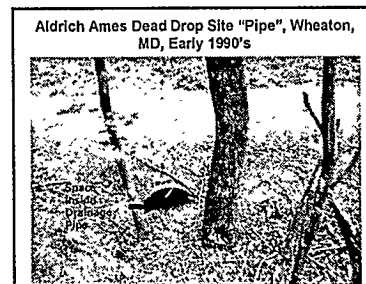
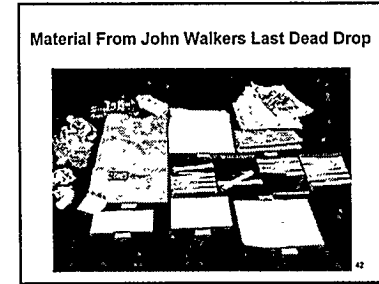
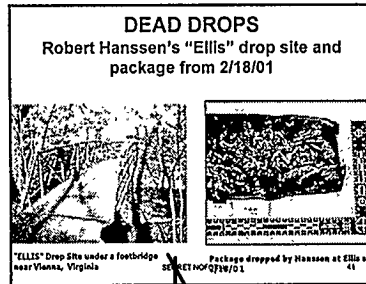
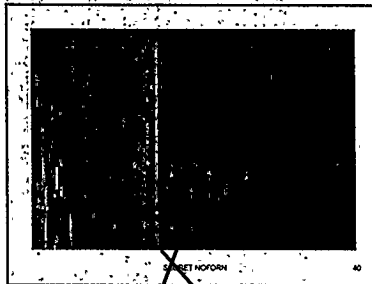
(S)

(S)

(S)



b1
b7E



~~SECRET~~

~~SECRET NOFORN~~

~~SECRET~~

~~SECRET NOFORN~~

(S)

(S)

[Redacted]

- **Photography**
 - Digital scanners
 - Mini cameras
 - Phone cameras
 - Digital cameras

~~SECRET NOFORN~~ 46

John Walker Demonstrates Document Photography



47

[Redacted]

- **Concealment Devices**
 - Quill pens during revolutionary war.
 - Coins, silver dollars, nickels.
 - Coke cans, shaving cream cans,

~~SECRET NOFORN~~ 48

b1
b7E

(S)

[Redacted]

~~SECRET NOFORN~~ 49

Brian Patrick Regan



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

(S)

(S)

~~SECRET NOFORN~~

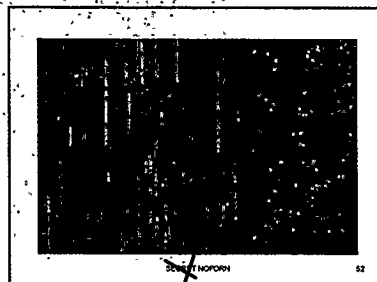
Miscellaneous

- One Time Cell Phones
- One Time Phone Cards
- Digital Scanner
- Cryptography

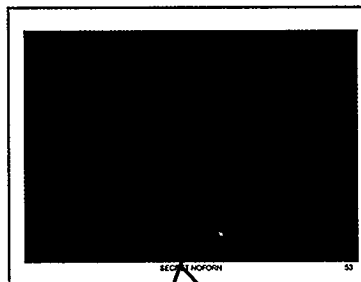
[Redacted]

~~SECRET NOFORN~~ 51

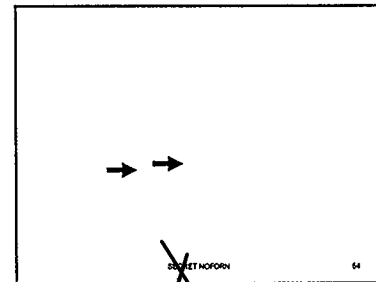
b1
b7E



52



53



54

~~SECRET~~

~~SECRET NOFORN~~

~~SECRET~~

~~SECRET NOFORN~~

(S)

~~SECRET NOFORN~~

Summary

- US considered the major leagues
- Their nation's best and brightest / trained and equipped

~~SECRET NOFORN~~ 55

~~SECRET NOFORN~~

Final Thoughts

- Universal Vs. Unique to Service
- Something unusual or not right – talk to SSGs, Senior Agents, HQ or CITC

~~SECRET NOFORN~~ 56

~~SECRET NOFORN~~

STEVE, SEEING YET ANOTHER OF HIS SECRET REPORTS LEAKED IN THE PRESS FOR THE THIRD TIME THIS WEEK, SUDDENLY REALIZED HE HAD BEEN THROWING HIS CLASSIFIED TRASH INTO THE DUMPER HE SHARED WITH THE WASH. INSTON POSTS STAR REPORTER WHO LIVED IN HIS CONDO COMPLEX.



~~SECRET NOFORN~~ 57

b1
b7E

~~SECRET NOFORN~~

Techniques

For Tuesday Practical Exercises

- Computer / Internet
- Library / Bookstores

~~SECRET NOFORN~~ 58

~~SECRET NOFORN~~

~~SECRET NOFORN~~ 59

~~SECRET NOFORN~~

Surveillance Practical

~~SECRET NOFORN~~ 60

b1
b7E

~~SECRET NOFORN~~

RULES OF ENGAGEMENT

- Teams should have an "eye" on the IO at all times.
- The eye will usually change when the IO enters a building or makes a turn.
- Because this is training the IO will not be overly sensitive to surveillance, however the Teams should be discreet.
- No "bumper lock" surveillance.

~~SECRET NOFORN~~ 61

~~SECRET NOFORN~~

Rules of Engagement

- The IO has the right to call a team member out of play if there is aggressive bumper lock surveillance
- This is a training exercise – an IO would NEVER conduct numerous acts in one outing.
- The goal is to observe as many acts as possible. Or be able to identify IO behavior which would lead you to believe a specific act was conducted.
- Mentors are to assist and observe

~~SECRET NOFORN~~ 62

~~SECRET NOFORN~~

Rules of Engagement

- Team that correctly identifies the most acts without getting a member taken out of play - Wins
- May the best team win

~~SECRET NOFORN~~ 63

~~SECRET~~

~~SECRET NOFORN~~

~~SECRET~~

~~SECRET NOFORN~~

(S)

SECRET NOFORN

EQUIPMENT

- Mail [redacted]
- Cell Phones
- Direct Connect Hand Held Radios
- Extra Batteries

SECRET NOFORN

(S)

(S)

[redacted]

- Cyber
 - Computer Intrusions
 - Encryption - e-mails
- [redacted]
- Digital Scanners
- One time disposable cell phones

[redacted]

SECRET NOFORN

(S)

(S)

(S)

SECRET NOFORN

Agent Communication

[redacted]

SECRET NOFORN

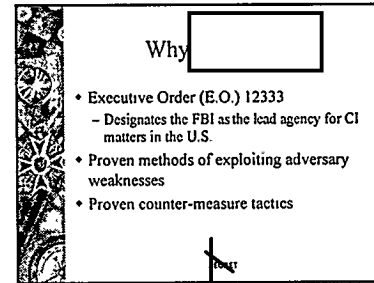
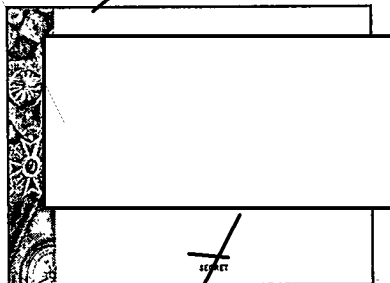
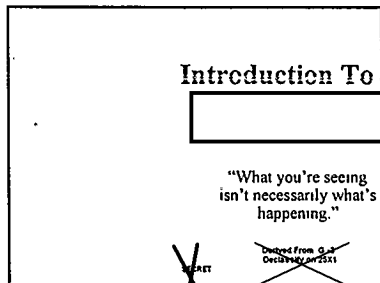
b1
b7E

~~SECRET~~

~~SECRET NOFORN~~

~~SECRET~~

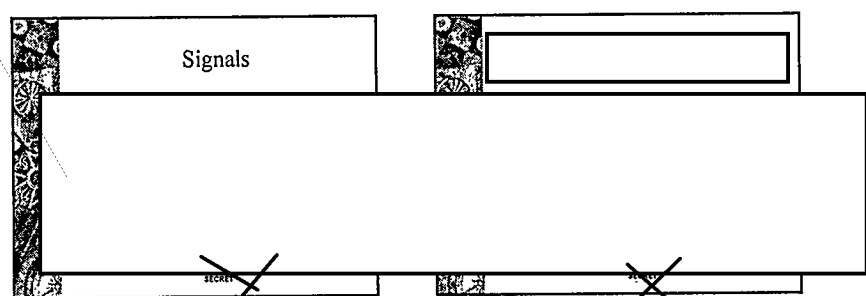
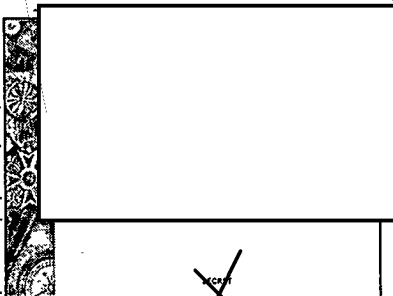
(S)



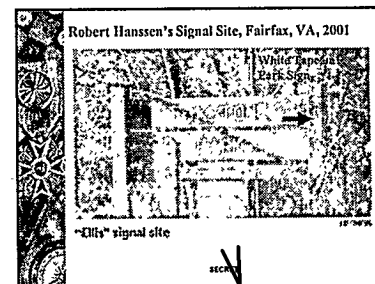
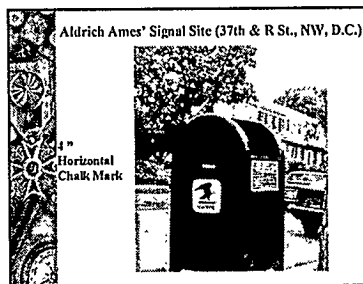
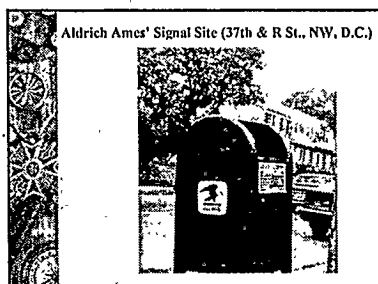
b1
b7E

(S)

(S)



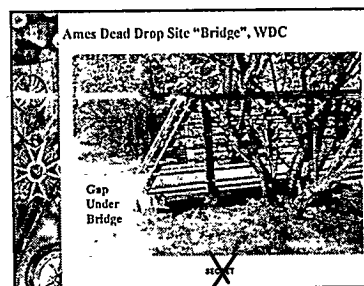
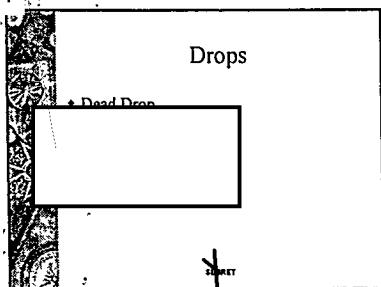
b1
b7E



~~SECRET~~

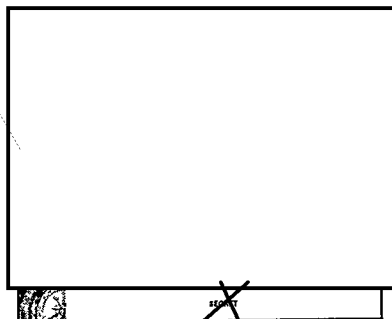
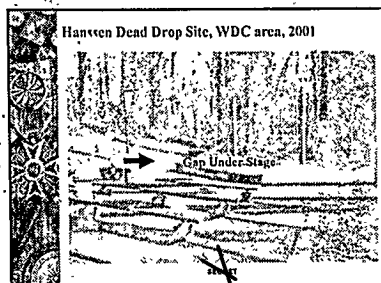
~~SECRET~~

(S)

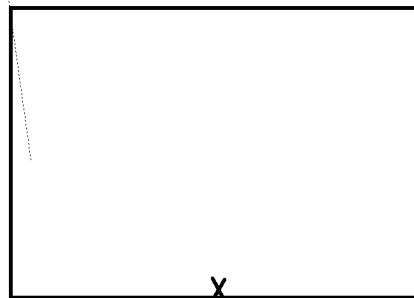


b1
b7E

(S)

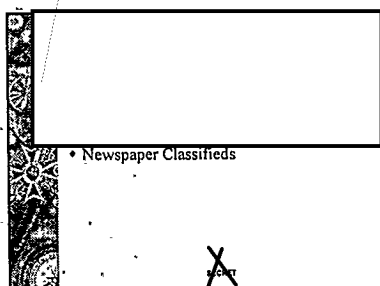


(S)

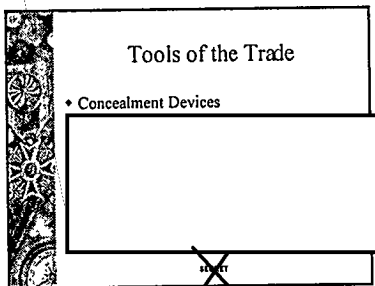


b1
b7E

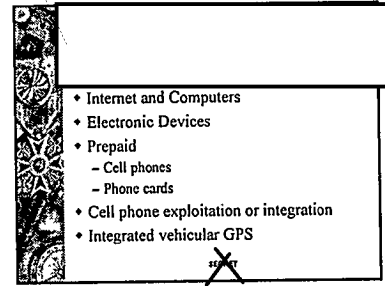
(S)



(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

(S)

(S)

(S)

Training

- Disguise
- Food & water

b1
b7E

(S)

(S)

- Brief Encounter

(S)

(S)

(S)

(S)

General Principles

• Are UNIVERSAL

b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(5)

(S)

(S)

(S)

(S)

(S)

(S)

(S)

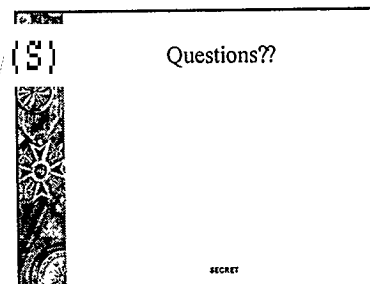
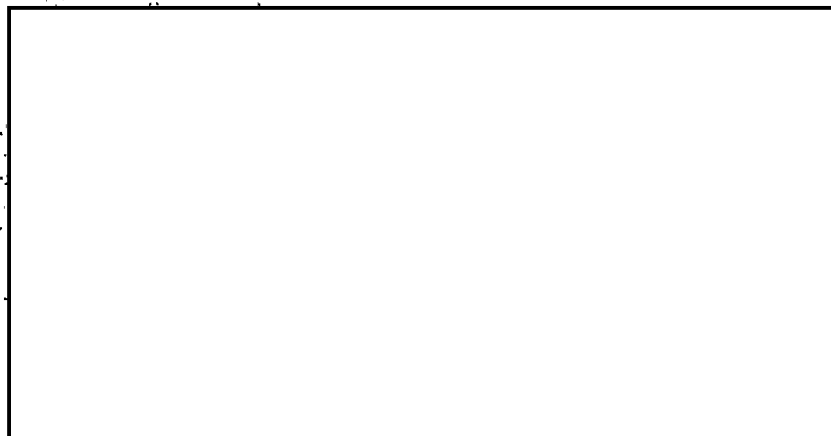
(S)

(S)

~~SECRET~~

(S)

b1
b7E



~~SECRET~~

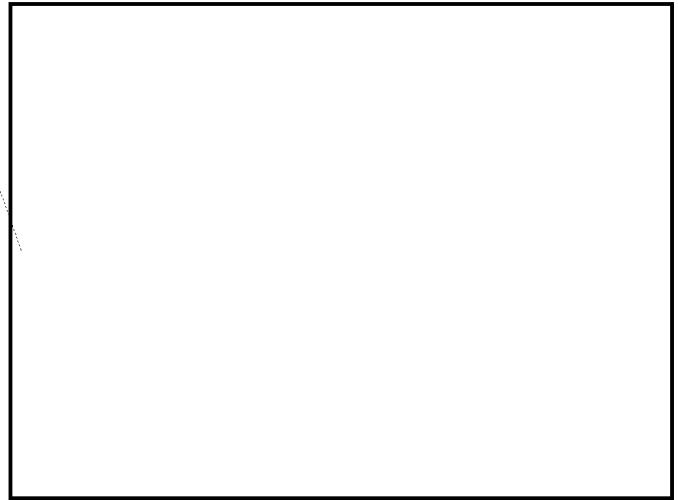
DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

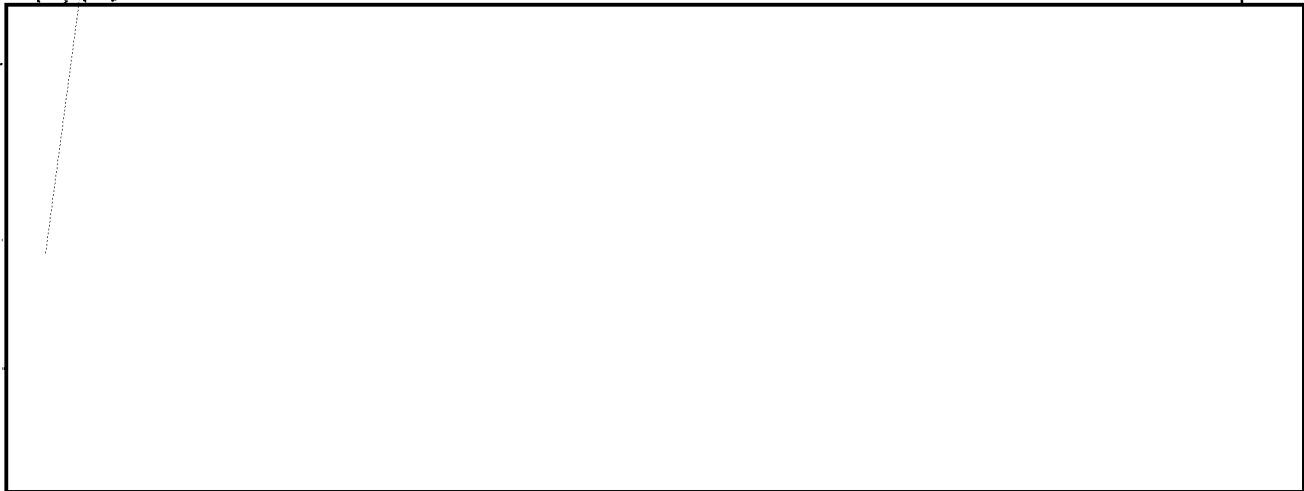
(S)

(S)



b1
b7E

(S)



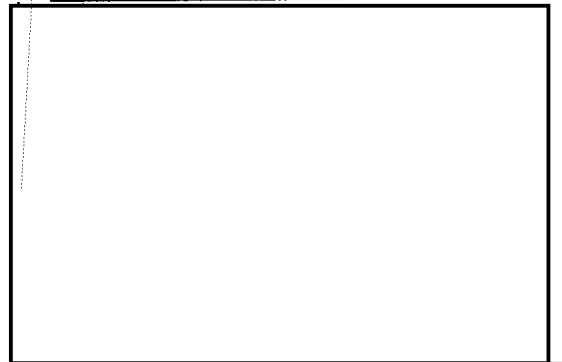
b1
b7E

(S)



(S)

FINAL THOUGHTS ...



b1
b7E

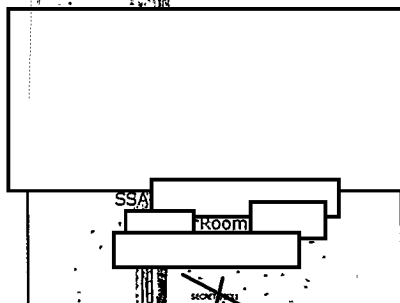
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

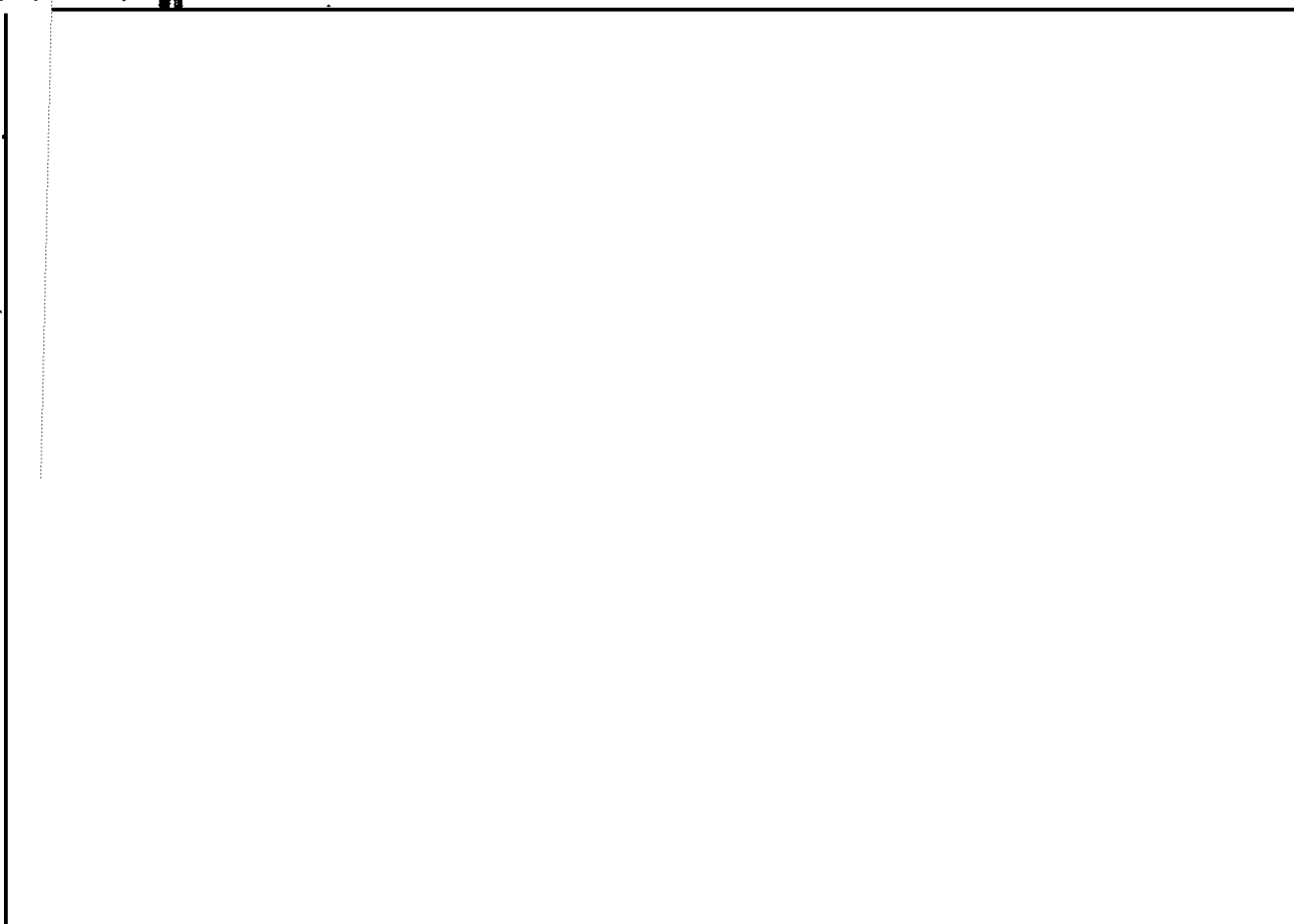


(S)



b1
b6
b7C
b7E

(S)



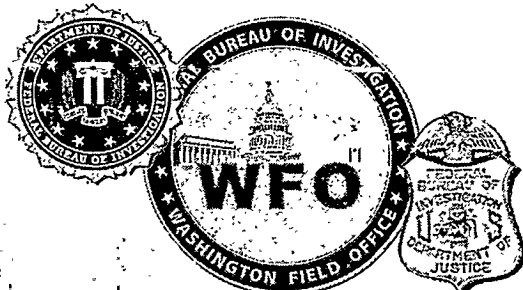
b1
b7E

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

F.B.I. AIR OPERATIONS



FEDERAL BUREAU OF INVESTIGATION

WFO

SSA
Full-time Pilots
Full-time FLIR
Operators



b7E

Who We Support

- SSG Teams
- SOG Teams
- Case Squads
- SWAT
- National Special Security Events
- Regional Support
- Aviation Surveillance Branch (ASB)

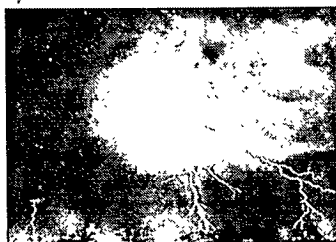
Capabilities

- 4+ hour on station surveillance
- Search/Arrest warrant support
- Counter-surveillance
- Forward Looking Infra-Red (FLIR)
- Day/Night video recording capability
- Real-time video downlink
- Radio relay
- Aerial photography

(S)

Limitations

- Visibility: Day vs. Night
- Crew day
- Waivers
- Weather
 - turbulence
 - clouds
 - precip: rain, snow, icing
- Wind
- Airspace



b1
b7E

~~SECRET~~

ACLURM043016

~~SECRET~~

Flight Schedule

	Pilot
	Co-Pilot
	Pilot
	Co-Pilot
FLIR	Pilot
	Co-Pilot
	FLIR Operator

Mission preparation:

- Contact Ground Team for location.
- Check current and forecast weather.
- Notify Air Traffic Control, U.S. Secret Service, Northeast Air Defense, U.S. Capitol Police and SIOC.
- Pre-flight aircraft.
- Start/Taxi/Takeoff & fly to working area.

b7E

Legal/Procedural

- ASAC approval for surveillance
- CDC approval for FLIR/Imaging

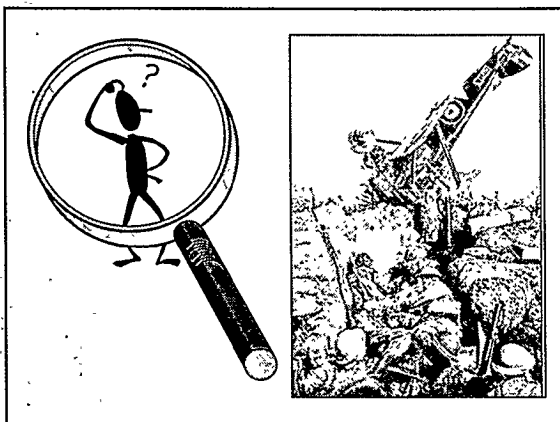
Point of Contact

Hangar at Manassas:

SSA



b6
b7C



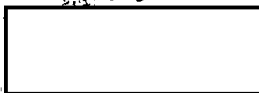
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Welcome To The World
Of



OBJECTIVES

OF THE

INVESTIGATION

OBJECTIVES

To Determine...

- > Whether a crime has been committed
- > What was lost...and how it was lost
- > Who committed the crime

b7E

OBJECTIVE

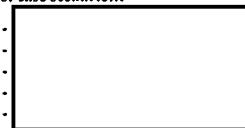
To make it believable to a jury
that a crime was committed,
and...

That the subject is the person who
committed the crime

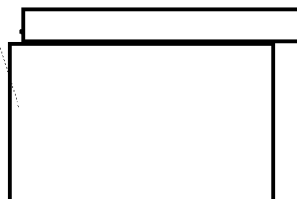
WHAT MAKES [REDACTED] CASES
SO DIFFICULT TO WORK?

(S)

Worst case scenario...



Where Do [REDACTED] Cases Come
From?



b1
b7E

WHAT DO WE NEED
TO
PROVE?

ELEMENTS OF THE CRIME

18 U.S.C. § 794(a)

Elements

- > Transmittal...of
- > National Defense Information (NDI)...to
- > A Foreign Power, or Agent thereof ...with
- > The Intent to injure the U.S. or aid the FP

(All elements of the statute must be met)

18 U.S.C. § 794(a)

Penalty

- > No statute of limitations
- > Death or life imprisonment
- > Criminal forfeiture provisions
- > "Son of Sam" provision

~~SECRET~~

ACLURM043018

~~SECRET~~

~~SECRET~~

**SATISFYING THE
ELEMENTS OF THE CRIME**

(what do we need to do?)

**ELEMENTS REQUIRING
CORROBORATION**

- > Transmittal...of
- > National Defense Information...to
- > A Foreign Power or Agent thereof...with
- > Intent to Injure the U.S. or Aid the FP

**KEYS TO SATISFYING THE
ELEMENTS**

Fix Guilt...

Elements of Crime

- Transmittal
- Foreign Nation/Agent
- National Defense
- Intent to Injure/Aid

Focus

Circumstances surrounding
message
and location
Fix on documents/info.
Info. that demonstrates intent

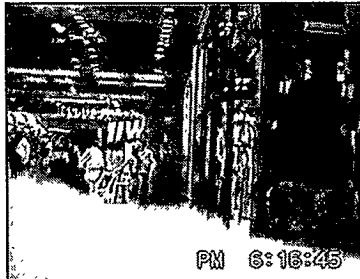
b1
b7E

ELEMENT - TRANSMITTAL

- (S)
- > Proof of opportunity to commit the crime
Follow document trail.
 - > Place of the location of transmittal

Transmittal area...
Location of transmittal(s)

ICB...
phone...
hotel...
written proposals/lists
employment...etc.



ELEMENT - NDI

- > Info relating to the national defense that is
appropriately, accurately and actually classified
- > Courts take liberal view of what constitutes NDI
- > Confidential, Secret, Top Secret (SCI)
- > Military, component parts

Documents...

- > Traceability / locatability
- > Access (direct or indirect)
- > Accountability / distribution / destruction

b1
b7E

(S)

ELEMENT

ELEMENT - INTENT

Three means to prove intent

- Inferred (indirect/circumstantial)
- Self-started
- Signed statement

ELEMENT - INTENT

Inferred...

- (S)
- > Proof of intent ("evil" if possible)
 - > A person is presumed to intend the natural and probable consequences of an act performed...a person's actions "speak" for them
 - > Actions, conduct, and comments offer evidence of intent
 - > Probe motivations
 - > Nature/classification/volume of information passed

b1
b7E

~~SECRET~~

~~SECRET~~

ELEMENT - INTENT

Self Stated...

- > Admits violation of security oath(s)
- > Discusses document selection criteria
- > Admits he knew info was accurately and appropriately classified at the time of passage
- > Admits value (usefulness) of info passed
- > Discusses ramifications of info passed
- > Discusses actions taken to avoid detection

ELEMENT - INTENT

Signed Statement...

- > Doesn't hold special significance/importance
- > A detailed FD-302 is usually better

(S) [Redacted]

(S) [Redacted] acted out)

LEGAL ISSUES

- Do you have PC? (Get it in writing!)
- Who has the lead?
- Coordinate with outside agencies...document!
- Do not let victim agencies lead!
- Joint interviews?
- Third agency rule - document authority to disseminate

b1
b7E

LEGAL ISSUES (Cont)

- CI language versus criminal

(S) [Redacted]

- Brady / Giglio / Garrity

QUESTIONS?

(S)

b1
b7E

1) Predication

- Referrals (US [Redacted])
- Coworkers/Neighbors
- Co-conspirators/Wives
- Polygraphs

2) Investigation

- Subject or Unsub
- Long term or Short term (as a spy)
- Active or Inactive (currently)
- Employed or Post employment

3) Interview / Interrogation

- Satisfy the elements of the crime
- Voluntariness (of the interview)

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

[Redacted]

4) Confession / Corroboration

- Worthless w/o corroboration
- Cannot stand on its own
- Believability/credibility
- May be required of successful prosecution

(S)

[Redacted]

5) Arrest

- You must be ready (at all times)
- Investigation does not stop
- You lose control (AUSA takes over)
- Confession before investigation
- Subject has "no right to be arrested!"
- (do it on your time frame when possible)

(S)

[Redacted]

6) Plea

- Ultimate goal
- No court
- No source issues
- No embarrassment

b1
b7E

(S)

[Redacted]

7) Trial / Conviction

- Brady / Giglio / Garrity
- Hearsay and analysis stop
- Slave to AUSA
- Keep list/copies of what provided

(S)

[Redacted]

8) Debriefing

- W, W, W, W, W, H
- Everyone wants a piece
- It's real work
- Audio tape

(S)

[Redacted]

9) Sentencing

- Have all the facts ready
- Statement of facts is power
- Breach of Trust

b1
b7E

(S)

[Redacted]

10) Damage Assessment

- Slave again
- Field will supply everything
- Keep list/copies of all you provide

Questions?

b1
b7E

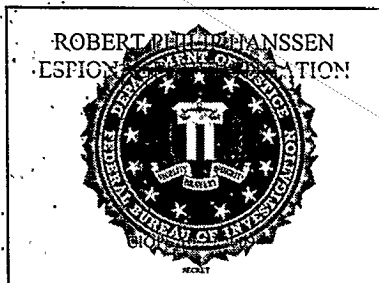
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

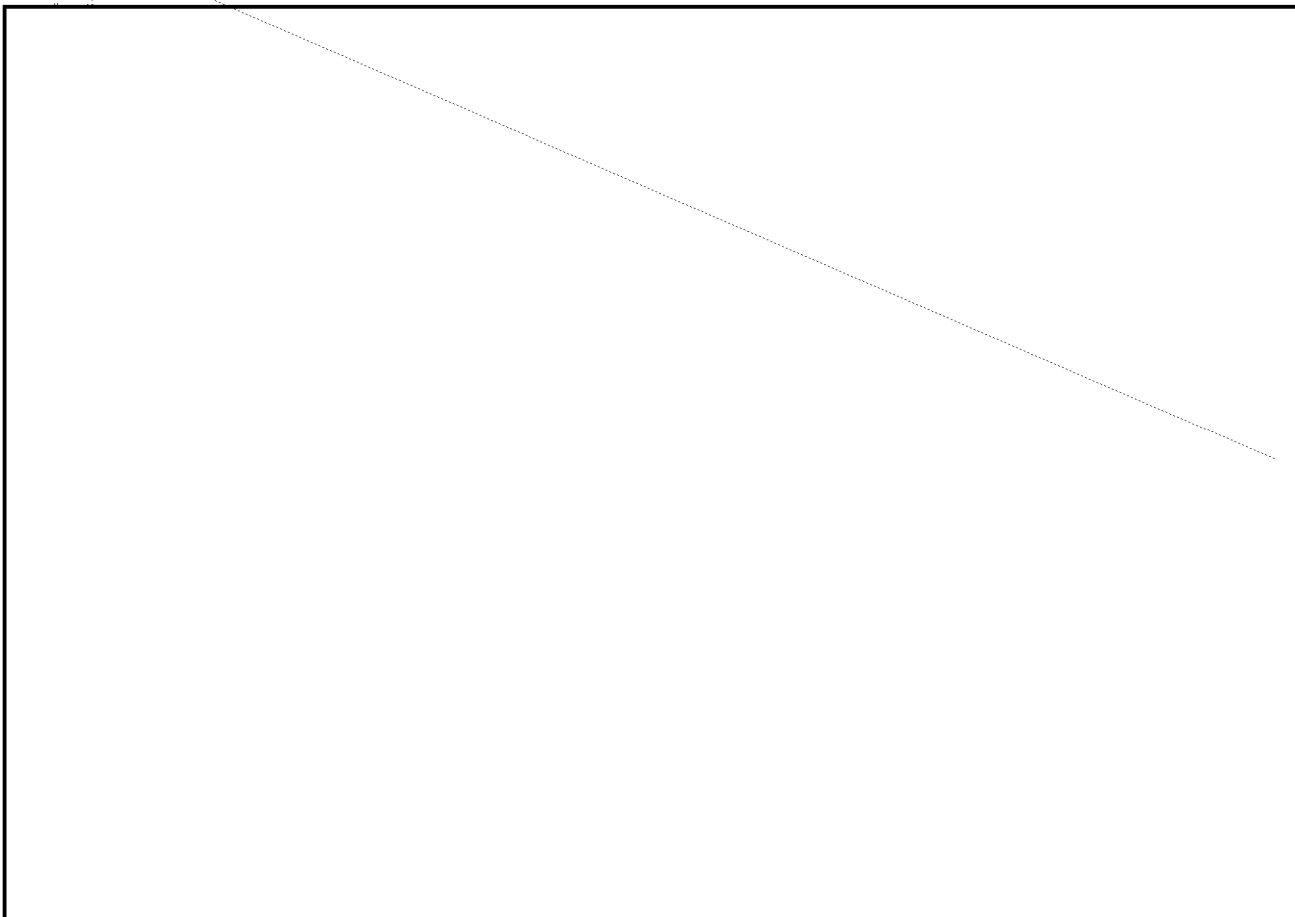
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)



b1
b7E

(S)

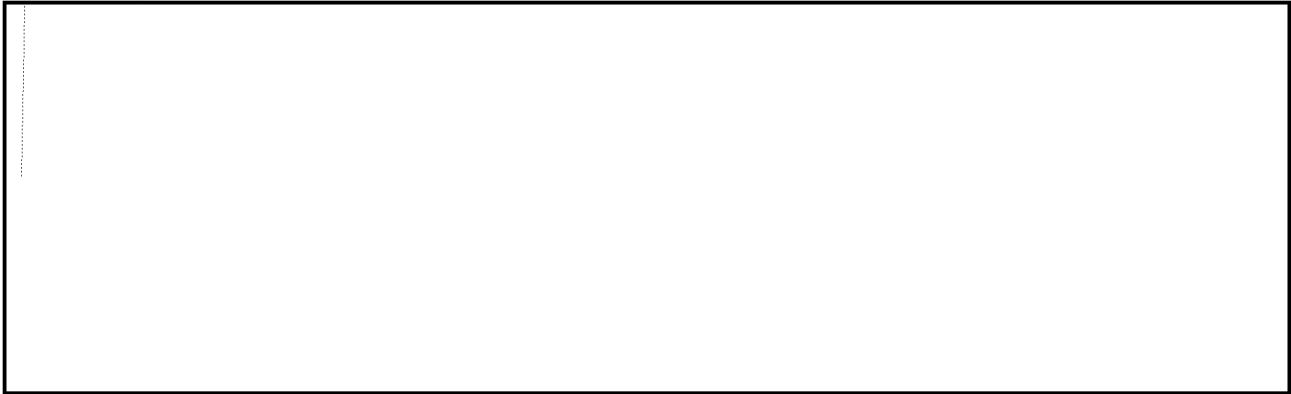


~~SECRET~~

ACLURM043022

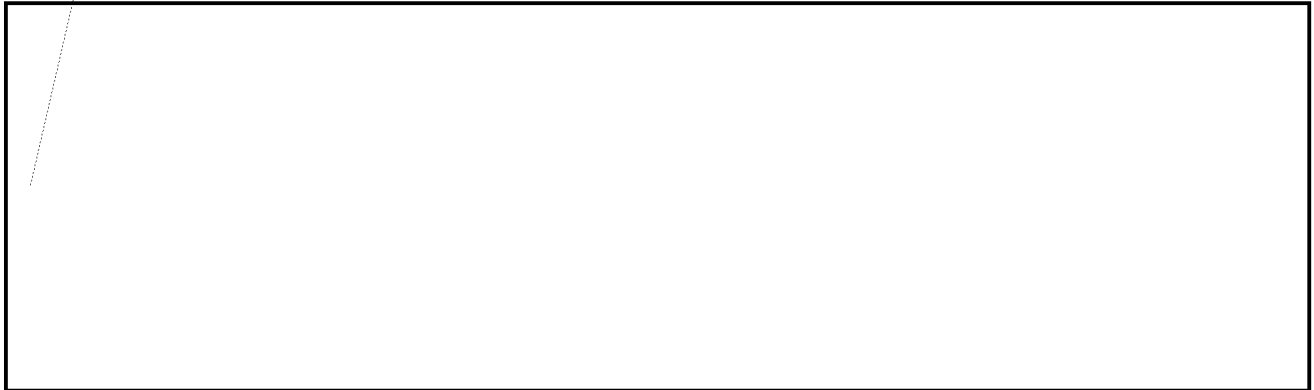
~~SECRET~~

(S)



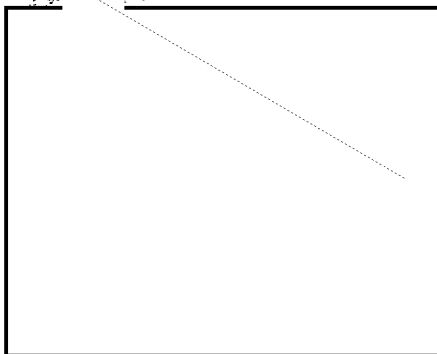
b1
b7E

(S)



b1
b7E

(S)



CONSIDERATIONS

- Was Hanssen still active
- Did Hanssen have any confederates
- Risk of flight
- Technical expertise
- Access to classified information
- ACS vulnerability
- Mandatory retirement April 18, 2001

Unclassified

GOAL

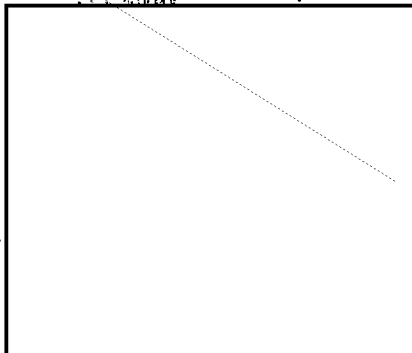
- Catch Hanssen in the act of committing espionage

Unclassified

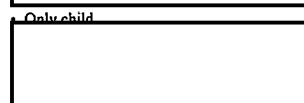
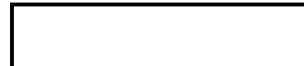
~~SECRET~~

~~SECRET~~

(S)



ROBERT P. HANSSEN



Unclassified

b1
b6
b7C
b7E

HANSSEN's EDUCATION

- A.B. Chemistry; Knox College, Galesburg, IL; 9/58-6/62
- Northwestern University Dental School, Chicago, IL; 9/66-10/68
- MBA Management Information Systems, Northwestern University, Chicago, IL; 9/69-6/71

Unclassified

HANSSEN PRE-FBI CAREER

- Illinois Department of Mental Health; Activities Worker, 1963-1966 (Summer)
- - HANSSEN m [redacted]
- Television Station WBBM-TV, Chicago, IL; Technician, 10/68-11/68
- Illinois Department of Mental Health; Social Worker 7/67-6/71

Unclassified

PRE-FBI CAREER CONT'D

- Touche, Ross & Co., Chicago, IL; Auditor (CPA); 6/71-10/72
- Chicago Police Department; Investigator; 10/72-12/75

Unclassified

b6
b7C

HANSSEN's FBI CAREER

- EOD FBI January 1976
- Indianapolis, Gary RA, April 1976-September 1978; White Collar Crime Squad, Accountant
- New York September 1978-January 1981
- White Collar Crime Squad, Accountant
- FCI Squad relief supervisor March 1979; works on Intelligence Information System

FBI CAREER CONT'D

- FBIHQ, INTD as SSA January 1981; [redacted]
- FBIHQ, INTD as SSA August 1983; [redacted]
- New York as SSA September 1985; [redacted]
- FBIHQ, INTD as SSA August 1987; [redacted]

~~SECRET~~

FBI CAREER CONT'D

- FBIHQ, Inspection Division, June 1990; Inspector's Aide
- FBIHQ, INTD June 1991; [redacted] Program Manager (scientific and technological CI)
- FBIHQ, INTD January 1992 as Unit Chief; [redacted]
- Washington Field April 1994; Phase II

~~SECRET~~

b7E

~~SECRET~~

~~SECRET~~

(S)

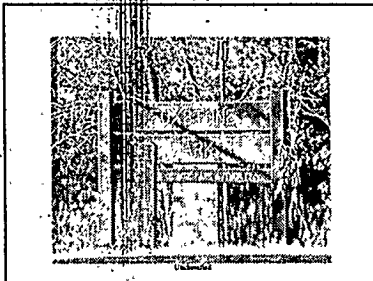
FBI CAREER CONT'D

- FBIHQ, NSD, December 1994; Front Office
- OFM/DOS, February 1995
- FBIHQ, IRD January 2001; Section Chief
- Arrested February 18, 2001
- Terminated from the FBI, February 23, 2001

4



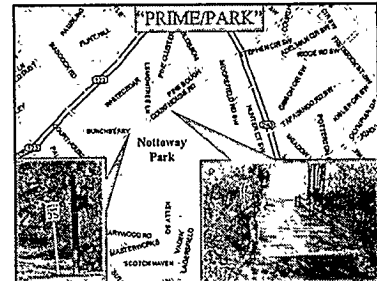
b1
b7E



RESULTS OF INVESTIGATION

- Review of HANSSEN's personnel file revealed HANSSEN previously resided within two blocks of Nottoway Park, codenamed PARK/PRIME

Unclassified



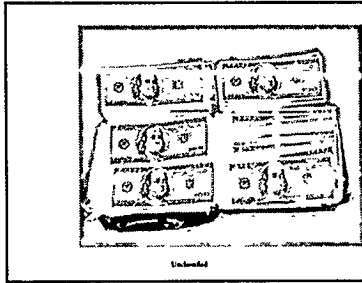
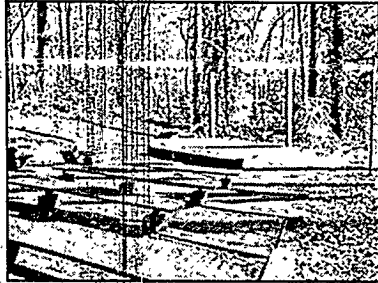
(S)



b1
b7E

~~SECRET~~

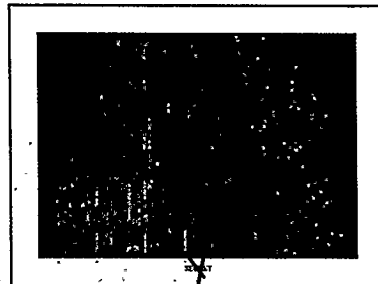
~~SECRET~~



THE ARREST

- HANSSEN was arrested on February 18, 2001 after he placed a package intended for the SVRR at Foxstone Park in Vienna, Virginia. The package included classified documents and a letter.

b6
b7C



The Letter

Dear Friend:

I thank you for your assistance these many years. It seems, however, that my greatest ability to you has come to an end, and it is time to recede myself from active service. Since communicating last, and one wonder if because of it, I have been promoted to a higher working level. I am now in the middle of regular reports to the Director while the counterintelligence program. It is as if I am being pulled. Furthermore, I have detected repeated bugging radio signal emanations from my radio. I have not found their source, but as you wisely do, I will leave this alone, for knowledge of their existence is sufficient. Amongst the power children play, in this, however, I strongly suspect you should have concerns for the integrity of your compartment concerning knowledge of my efforts on your behalf. Something has aroused the sleeping tiger. Perhaps you know better than I life is full of traps and dangers. My hope is that, if you respond to this constant confidential contact message, you will have provided some sufficient means of freedom besides it. If not, I will be in contact next year, same time same place. Perhaps the correction of forces and circumstances will allow me to reach my friend,

POST ARREST INVESTIGATION

- Interviews
- Financial Analysis
- Document Review
- Audit of Information Systems
- Analytical Effort
- Review of Evidence
 - Computers and computer media

POST ARREST INVESTIGATION

- An interview [redacted] revealed that HANSSEN may have committed espionage as early as 1979
- An interview of [redacted] that she loaned HANSSEN over \$95,000 during the 1990's
- HANSSEN had a Swiss bank account

POST ARREST INVESTIGATION

- HANSSEN had a relationship with an exotic dancer

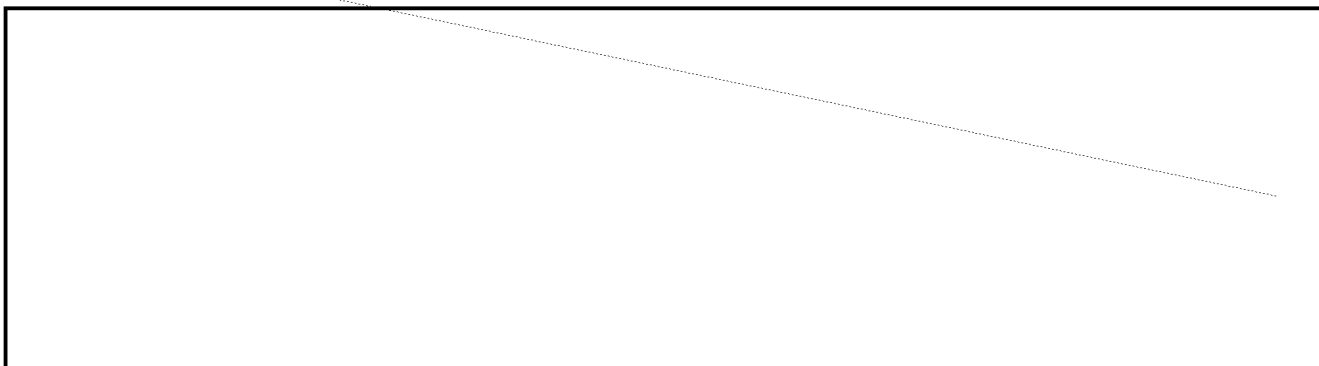
b1
b6
b7C
b7E

~~SECRET~~

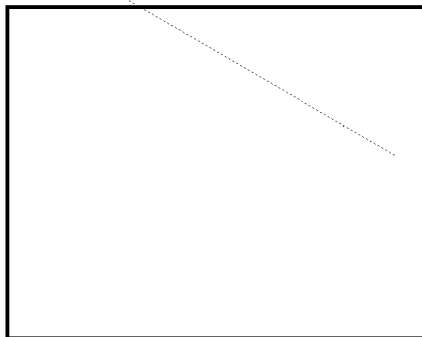
~~SECRET~~

b1
b7E

(S)



(S)



(S)

OUTCOME

- Plea agreement reached
 - two four hour proffer sessions
 - HANSSEN agreed to full, honest, and complete debriefing sessions with USIC
 - no pursuit of death penalty-BEST INTEREST OF NATIONAL SECURITY
- [redacted] receives survivor benefits of HANSSEN's retirement

Unclassified

b1
b6
b7C
b7E



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

(S)



b1
b7E

(S)



SENTENCING

- Sentenced on May 10, 2002 to life in prison without the possibility of parole
- Incarceration governed by Attorney General mandated Special Administrative Measures

Unclassified

SPECIAL ADMINISTRATIVE MEASURES

- "Based upon information provided to me, I find that [redacted] on Hanssen are reasonably necessary to prevent disclosure of classified information, that there is danger Hanssen will disclose such information, and that the unauthorized disclosure of such information would pose a threat to the national security of the U.S."

Unclassified

SPECIAL ADMINISTRATIVE MEASURES

- Attorney Visits
- Contemporaneously Monitored Family Visits
 - No contact
- Contemporaneously Monitored Telephone Calls-family and attorney only
- Mail-family and attorney only

Unclassified

HANSEN QUOTES

- "Frustrating not being able to help. The attacks were reported during my debriefing and we shut down. All the agents had to go back to help. I felt like, 'Hey, what about me.' I have all the training and skills, etc., but such is the sorrowful reality of squandering trust."

Unclassified

b6
b7C

~~SECRET~~

~~SECRET~~

HANSSSEN QUOTES

- "By focusing now on what was our worst counterintelligence failure, perhaps we can gain a counterterrorism victory."

Unclassified

BOOKS

- Robert Philip Hanssen, The Most Dangerous Double Agent in FBI History by David Wise (2001)
- The Spy Who Stayed Out in The Cold: The Secret Life of FBI Double Agent Robert Hanssen by Adnan Havill (2002)
- The Spy Next Door: The Extraordinary Life of Robert Philip Hanssen, The Most Damaging FBI Agent In US History, by Elaine Shannon and Anne Blackman (2002)

Unclassified

BOOKS

- Spy. The Inside Story of How the FBI's Robert Hanssen Betrayed America by David Wise (2003)
- Into The Mirror: The Life of Master Spy Robert P. Hanssen by Lawrence Schiller (2004)
- Spy Handler: Memoir of a KGB Officer The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames by Viktor Cherkashin (2005)

Unclassified

"This is punishment...."

SUPERMAX, Florence, Colorado

August 1, 2002



QUESTIONS?

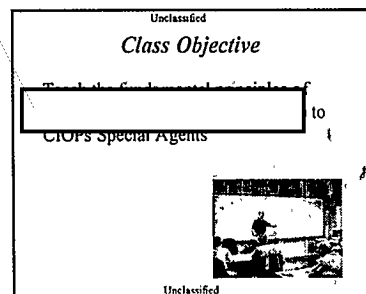
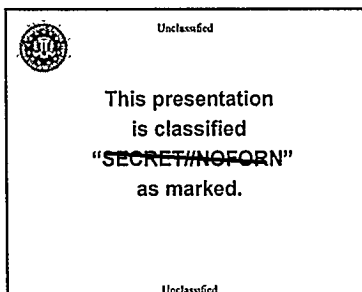
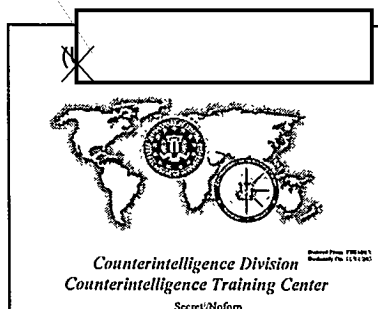
~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

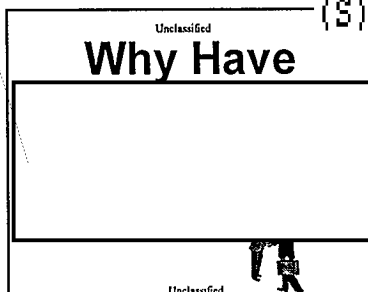
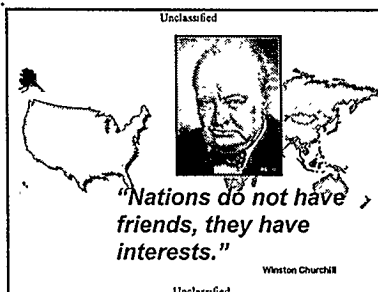
(S)



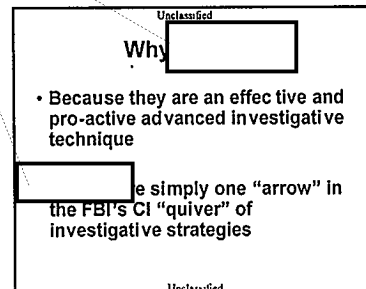
b1
b7E

(S)

(S)



(S)

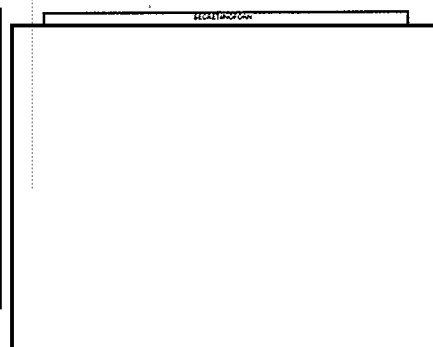
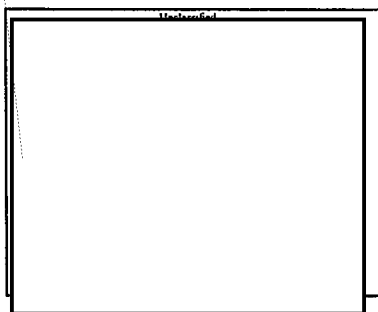


b1
b7E

(S)

(S)

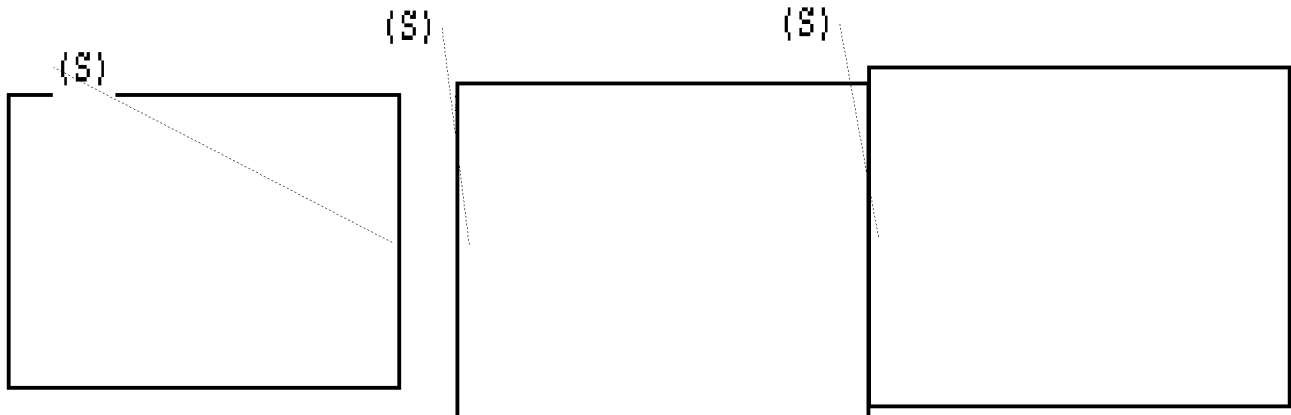
(S)



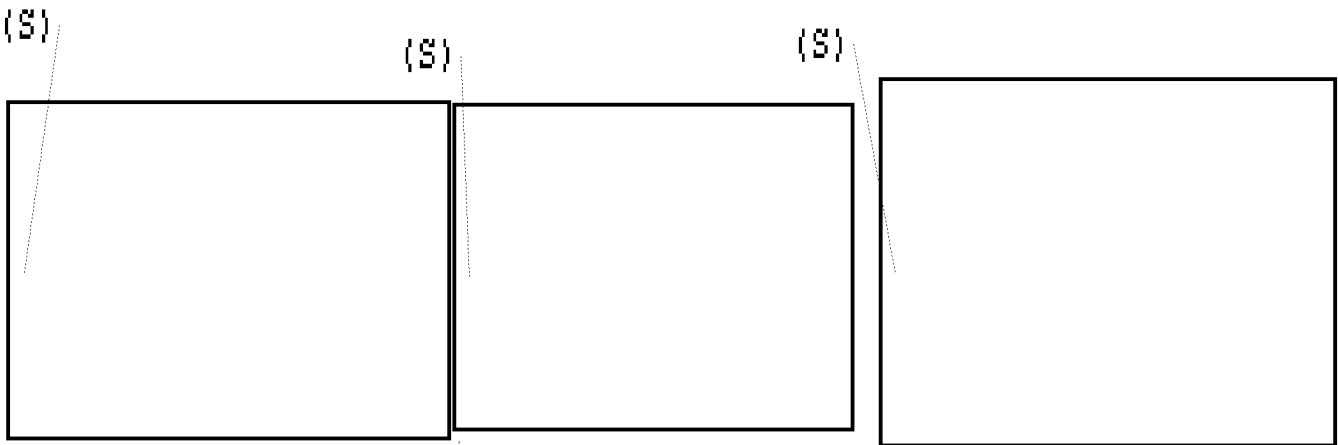
b1
b7E

~~SECRET~~

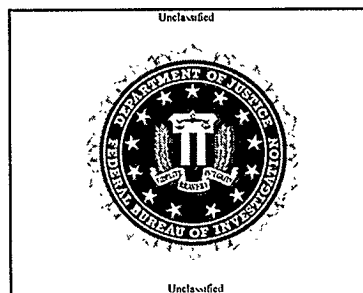
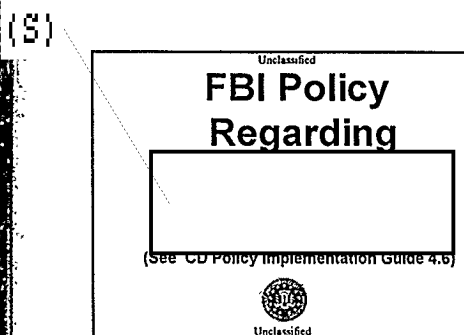
~~SECRET~~



b1
b7E



b1
b7E



b1
b7E

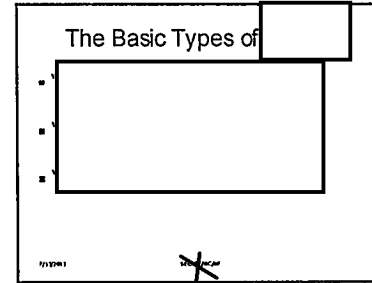
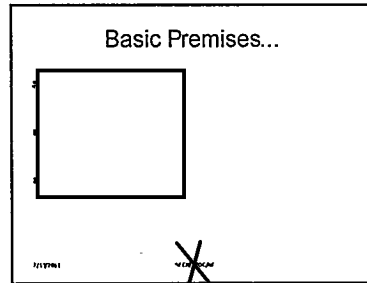
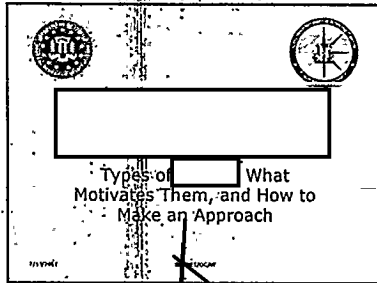
~~SECRET~~

DATE: 02-17-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-17-2037

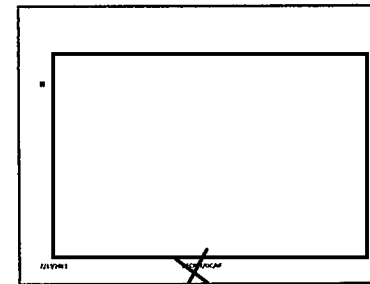
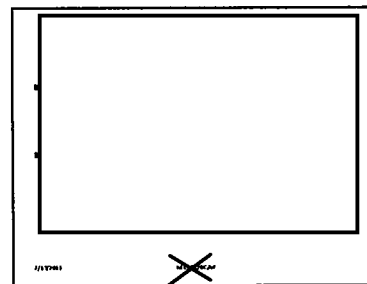
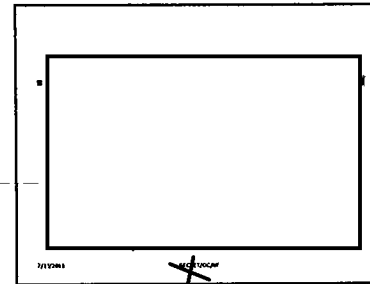
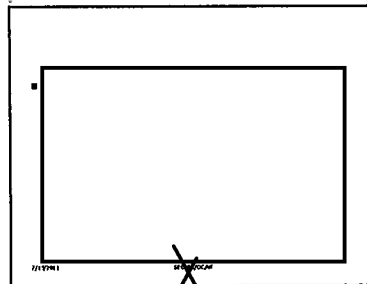
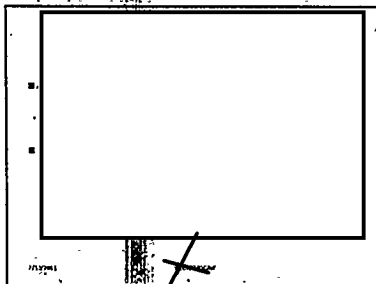
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b7E



b7E



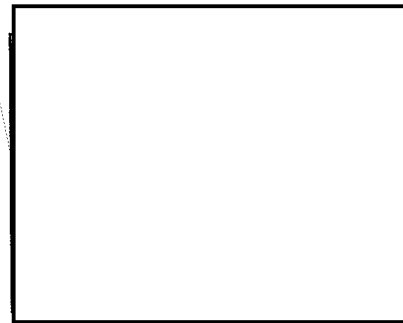
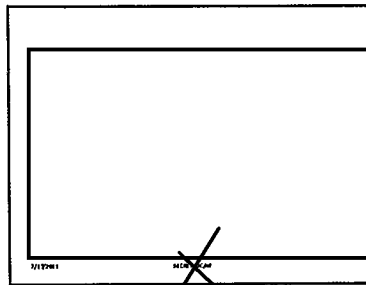
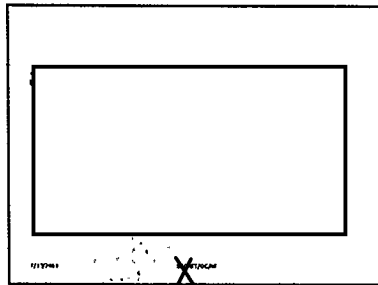
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

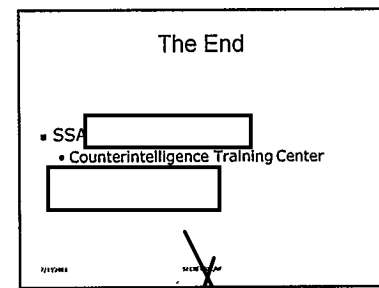
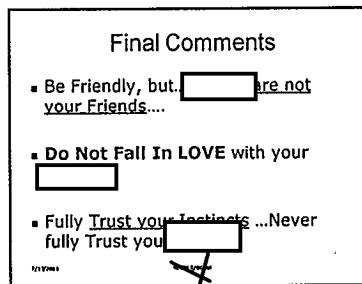
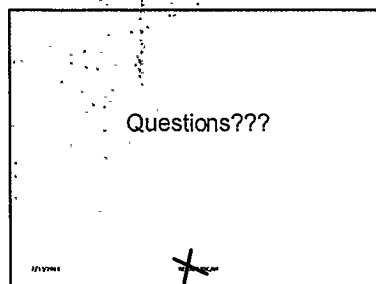
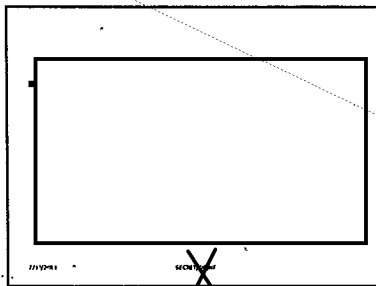
(S)



(S)

b1
b7E

(S)



b6
b7C
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

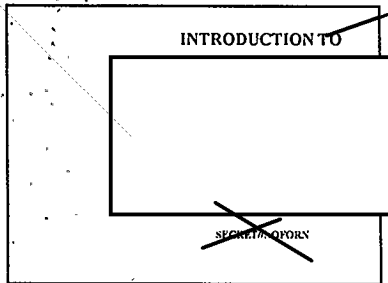
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET // NOFORN~~

~~SECRET~~

(S)

(S)



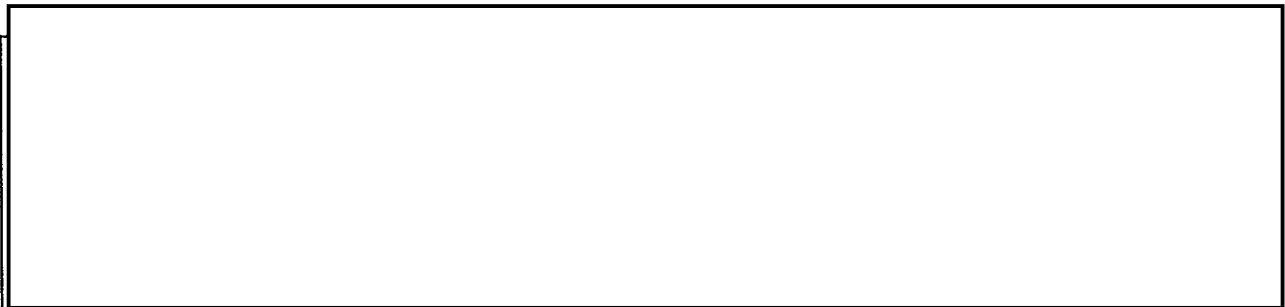
b1
b7E

(S)



b1
b7E

(S)



b1
b7E

~~SECRET~~

~~SECRET // NOFORN~~

ACLURM043034

~~SECRET~~

~~SECRET~~ // NOFORN

(S)

(S)

b1
b7E

(S)

The Answer: YES!

~~SECRET~~ // NOFORN

~~SECRET~~ // NOFORN

(S)

b1
b7E

(S)

~~SECRET~~ // NOFORN

~~SECRET~~ // NOFORN

~~SECRET~~ // NOFORN

b1
b7E

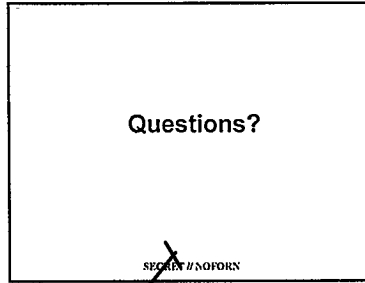
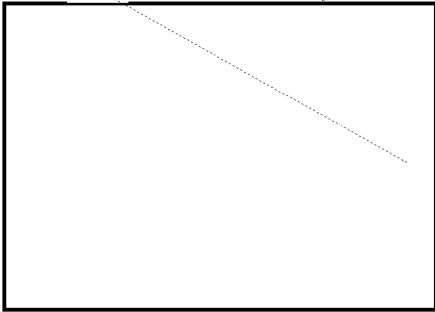
~~SECRET~~

~~SECRET~~ // NOFORN

~~SECRET~~

~~SECRET~~ // NOFORN

(S)



Questions?

~~SECRET~~ // NOFORN

b1
b7E

~~SECRET~~

~~SECRET~~ // NOFORN

ACLURM043036

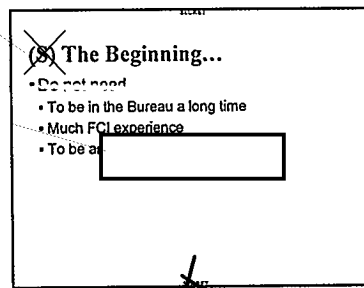
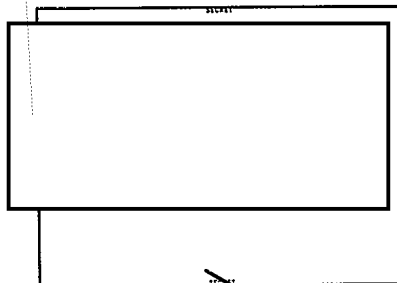
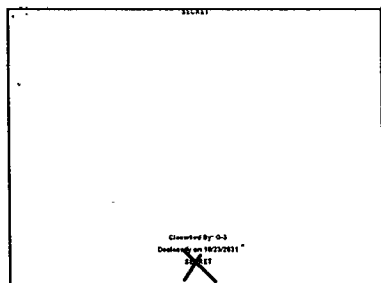
DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(U)

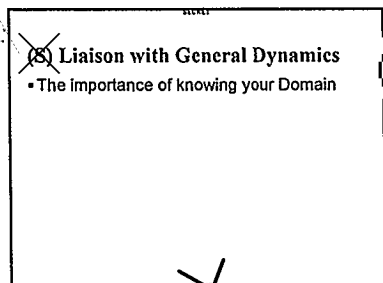


b1
b7E

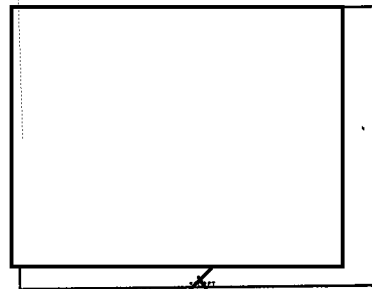
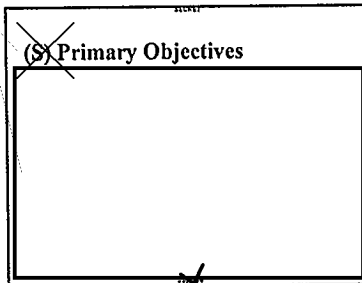
(U)

(U)

(S)



(S)

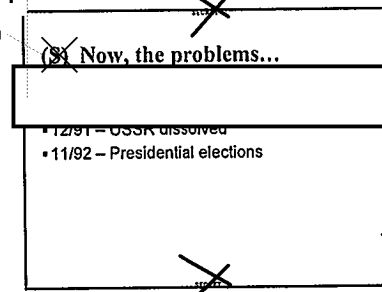
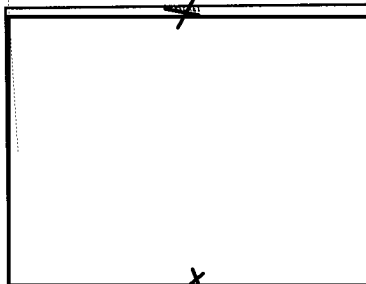
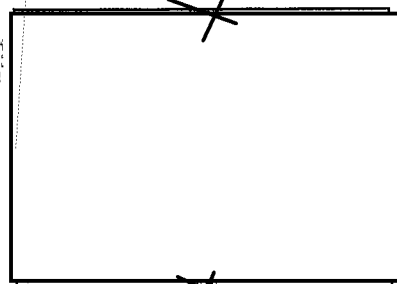


b1
b7E

(S)

(S)

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

(U)

(S)

~~(S)~~ Bottom Line

- Over three years from case initiation to initial contact (5/90 - 7/93)

Be Patient...

- On matters over which you have control
- Once operation gets started, some of that control may be lost

b1
b7E

(S)

(S)

(S)

b1
b7E

(S)

(S)

(S)

b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

(S)

~~(S)~~ Objectives Achieved

(S)

Questions?

2) Objectives Achieved:

- The following objectives were achieved:
- The following objectives were achieved:
- The following objectives were achieved:
- The following objectives were achieved:
- The following objectives were achieved:
- The following objectives were achieved:

~~SECRET~~

DATE: 02-15-2012

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

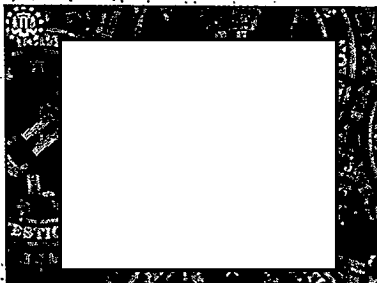
DECLASSIFY ON: 02-15-2037

ALL INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

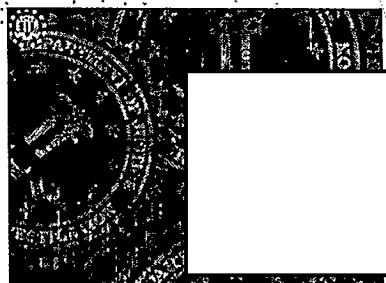
DATE 02-05-2012 BY 65179 DMH/STW

~~SECRET~~



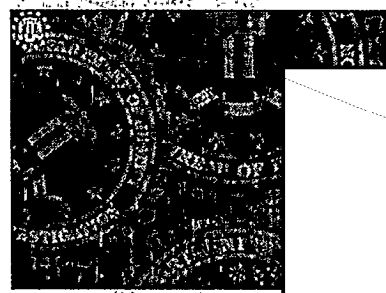
b6
b7C
b7E

(S)



b1
b6
b7C
b7E

(S)



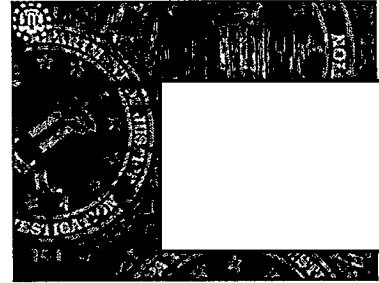
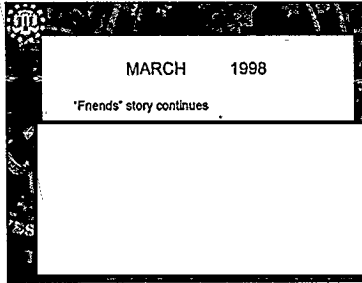
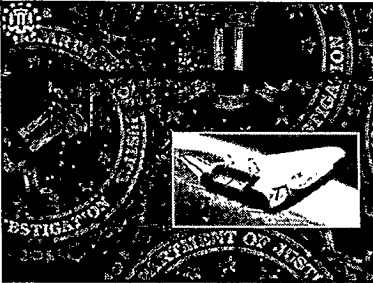
b1
b6
b7C
b7E

~~SECRET~~

ACLURM043040

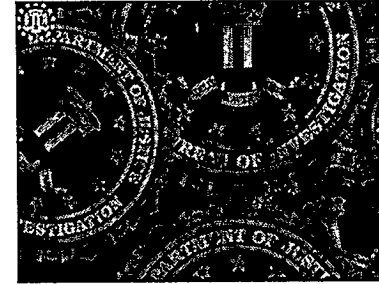
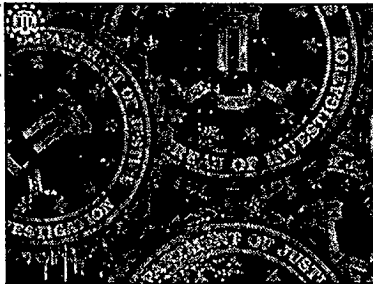
~~SECRET~~

(S)



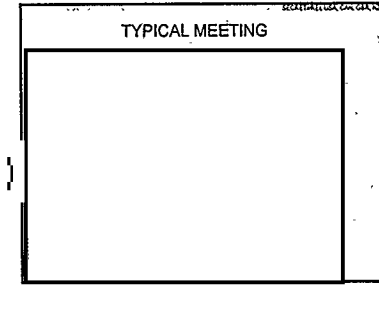
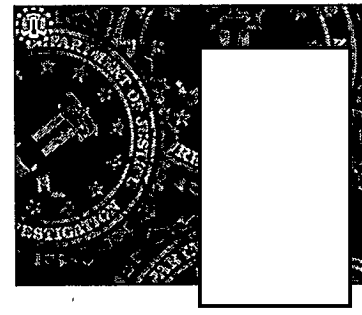
b1
b6
b7C
b7E

(S)



b1
b7E

(S)

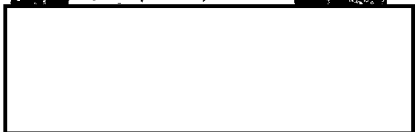
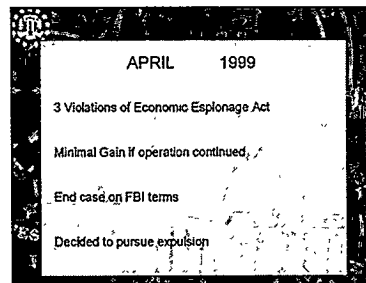
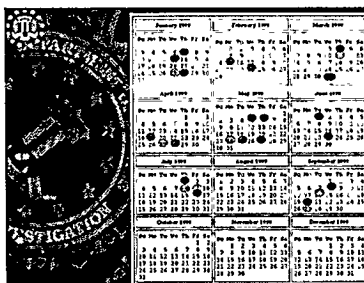
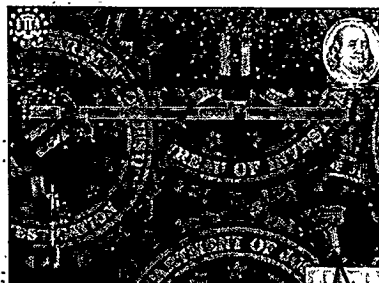


(S)

b1
b6
b7C
b7E

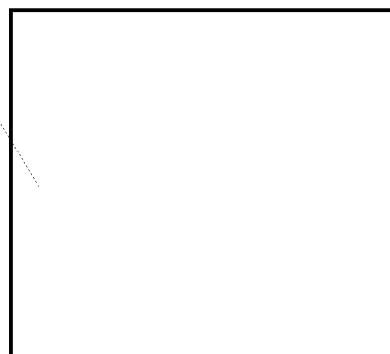
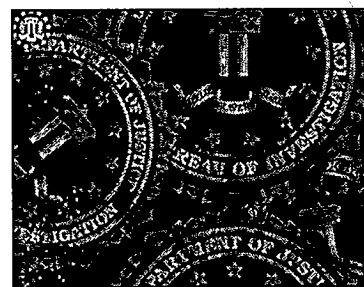
~~SECRET~~

~~SECRET~~



b6
b7C
b7E

(S)



b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

(S)



b1
b6
b7C
b7E

(S)

(S)

b1
b6
b7C
b7E

(S)

b1
b6
b7C
b7E

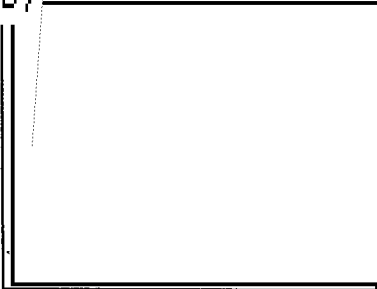
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

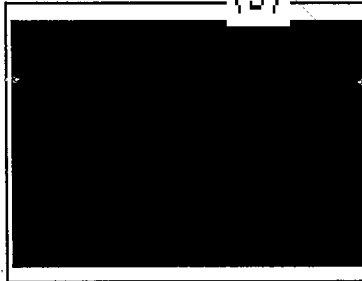
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

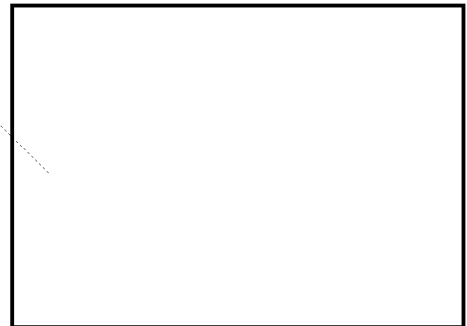
(S)



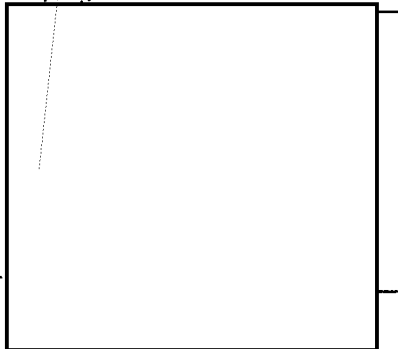
(S)



b1
b7E



(S)



(S)

What Do We Wish To Accomplish?

- 1) Create a notional current situation...
- 2) Providing a pose which facilitates...
- 3) A discussion of the recent offer or past activity...

b1
b7E



(S)

What we need to do?

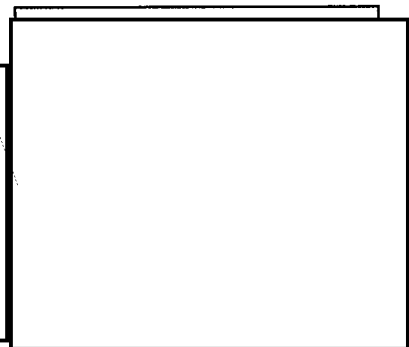
A rectangular box that has been completely redacted, appearing as a solid white area.

(S)

> Understand the subject

A rectangular box that has been completely redacted, appearing as a solid white area.

(S)



b1
b7E

~~SECRET~~

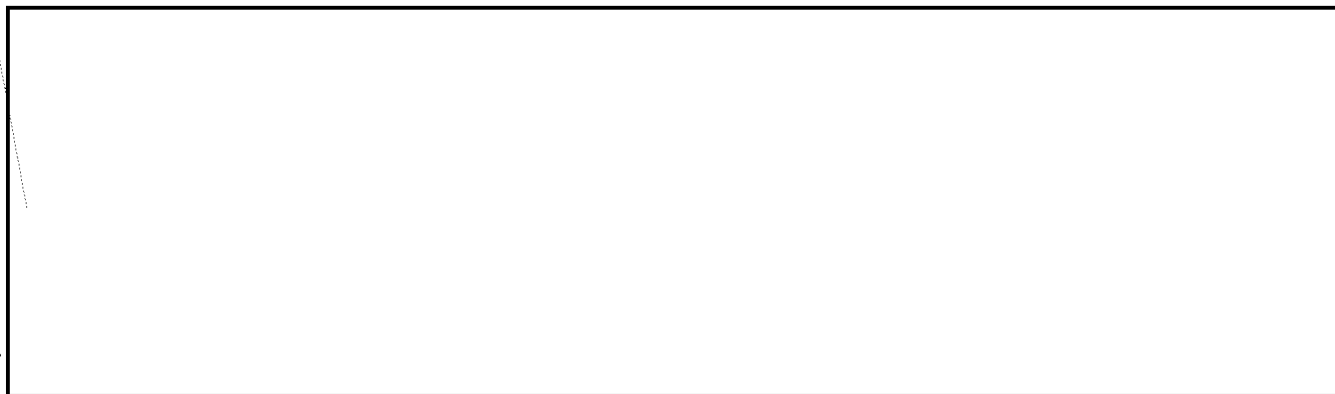
~~SECRET~~

(S)

(S)



(S)



b1
b7E

(S)



QUESTIONS?

~~SECRET~~

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

~~SECRET//NOFORN~~

FBI Counterintelligence
Division

Program Managed by [REDACTED]

The overall classification of this briefing is ~~SECRET//NOFORN~~
Unmarked bullets are UNCLASSIFIED
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

The Situation

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

The Situation

We have what they want...
...and they know it...
...because we collaborate with them...
...and welcome them with open arms

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

The Situation:

(S)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

b1
b7E

(S)

~~SECRET//NOFORN~~

(S)

(S)

~~SECRET//NOFORN~~

- Protect our sensitive national resources
- Stop illegal acquisition of protected technology by foreign powers which could harm national security
- Identify the insider threat

~~SECRET//NOFORN~~

(S)

(S)

(S)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

b1
b7E

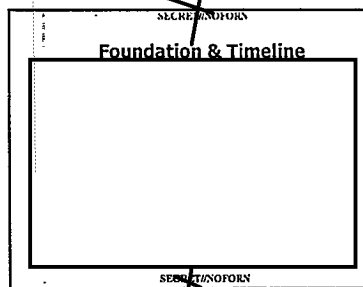
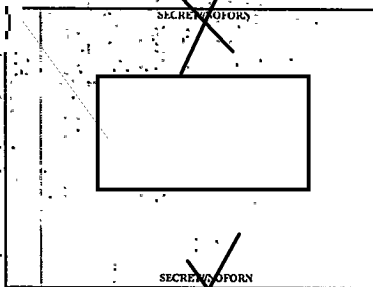
~~SECRET~~

~~SECRET~~

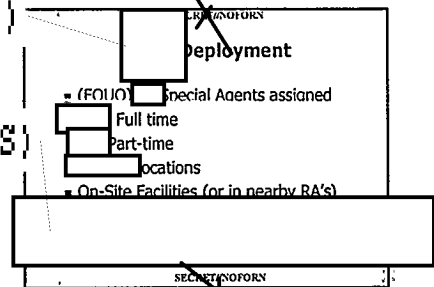
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)

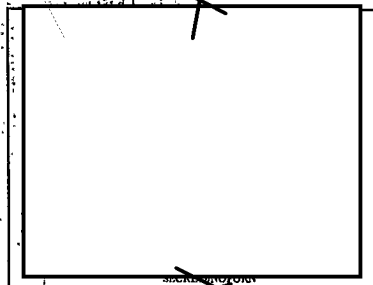


(S)

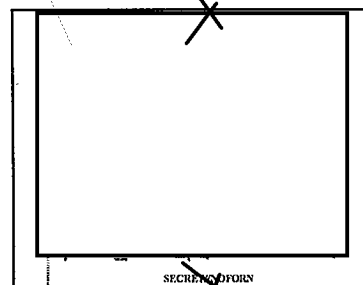


b1
b7E

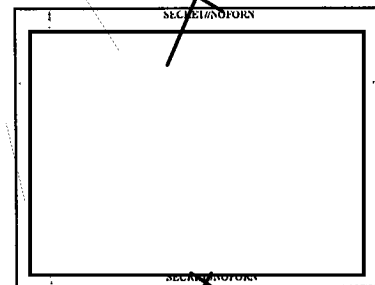
(S)



(S)

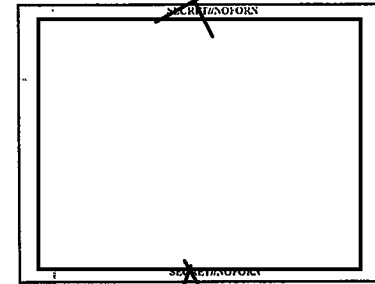
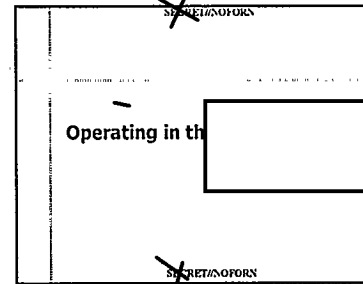
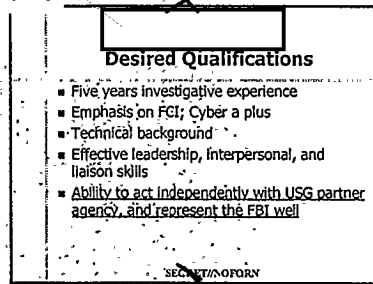


(S)



b1
b7E

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

~~SECRET//NOFORN~~

A Word about [redacted]

- Highly skilled personnel
 - Comprised of veteran FBI, OSI, etc personnel
- Small but highly proficient
 - Limited authorities under E.O. 12333
 - Relies on referrals to FBI
- Remember: still a competing USG agency
 - Different objectives/agenda
 - Different political considerations/constraints

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

What an FBI Agent needs to know

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

What you need to know if [redacted] in your backyard

- Sooner or later something related to [redacted] will cross your desk
- All FBI domains have universities/colleges that likely have engineering/sciences schools
 - US technology "out-sourced"
- Scientists move around/extensive interaction/seek peer review/foreign travel
- Another resource: CARDS, IIRs, Threat Assessments

~~SECRET//NOFORN~~

(S)

(S)

(S)

~~SECRET//NOFORN~~

Working with [redacted]

- Contact the local [redacted] FCI or Domain Squads
- [redacted] has excellent working relationships with FBI
 - Work with [redacted] to get access
 - No front coordination is the name of the game
- Know [redacted] environment and its challenges
- NR is likely there as well so factor them in

~~SECRET//NOFORN~~

(S)

(S)

(S)

~~SECRET//NOFORN~~

[redacted]

[redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

[redacted]

FBIHQ PM

MAPA

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

QUESTIONS?

~~SECRET//NOFORN~~

~~SECRET~~

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

DATE: 02-15-2012

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

DECLASSIFY ON: 02-15-2037 (S)

~~SECRET//NOFORN~~

(S)

**FDI Counterintelligence
Division**

[Redacted]

Program Managed by [Redacted]

The overall classification of this briefing is
~~SECRET//NOFORN~~
Unmarked bullets are UNCLASSIFIED
~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Overview

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Overview (Cont'd)

[Redacted]

b1
b7E

(S)

~~SECRET//NOFORN~~

Mission

- Protect our sensitive national resources
- Stop illegal acquisition of protected technology by foreign powers which could harm national security
- Identify the insider threat

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

The History

- 1999-2000 [Redacted]
- 2001: DOJ Bellows Report [Redacted]
- Aug 2001 [Redacted] Program Established
- [Redacted] Permanent [Redacted]
- Jun 2004 [Redacted] Program Expanded
- [Redacted] Addition [Redacted]
- [Redacted] Pilot [Redacted] [Redacted]
- 2004-Pres. [Redacted]
- 2006-Pres. Program Mature, Planning [Redacted]

~~SECRET//NOFORN~~

b1
b7E

(S)

~~SECRET//NOFORN~~

[Redacted]

- (FOUO) [Redacted] Special Agents assigned
- [Redacted] Full time
- [Redacted] Part-time
- [Redacted] Locations
- On-Site Facilities (or in build-out)

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

~~SECRET//NOFORN~~

Desired Qualifications

- Five years investigative experience
- Emphasis on FCI; Cyber a plus
- Technical background
- Effective leadership, interpersonal, and liaison skills
- Ability to act independently with USG partner agency, and represent the FBI well

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

What does a [redacted] Agent Do?

- Investigations – all varieties including 65 matters
- Liaison

[redacted]

- Daily Challenges
 - American/scientific community openness
 - DOE Culture: Science vs. Security
 - Egos & personalities
 - Balancing additional requirements of field office

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[redacted]

~~SECRET//NOFORN~~

b1
b7E

(S)

~~SECRET//NOFORN~~

A Word about [redacted]

- Highly, highly experience
 - Comprised of veteran FBI, OSI, etc personnel
 - Solid analytical capability (some member ~ IIRs)
 - Access to technical/subject matter experts
- Small but highly proficient
 - Limited authorities under E.O. 12333
 - Relies on referrals to FBI
- Remember: still a competing USG agency
 - Different objectives/agenda
 - Different political considerations/constraints

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Why should an FCI Agent Care?

- Sooner or later something related [redacted] will cross your desk
- All FBI domains have universities/colleges that likely have engineering/sciences schools
 - US technology "out-sourced"
 - Scholars/Researchers/Visitors/Conferences
 - [redacted] Scientists move around/engage interaction/seek peer review/foreign travel
- Another resource: CARDS, IIRs, Threat Assessments

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[redacted]

~~SECRET//NOFORN~~

b1
b7E

(S)

~~SECRET//NOFORN~~

[redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

Prominence with FBI Decision Makers

"We have focused on working with those who may be targets of foreign counterintelligence efforts... We implemented an "Agents in the Lab" program in specific DOE facilities for the purpose of raising counterintelligence awareness and broadening the FBI's access to intelligence within the labs."

- Robert S. Mueller III
FBI Director

Written Statement before House Appropriations Subcommittee on Science, the Departments of State, Justice and Commerce, and Related Agencies, September 14, 2004.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

[redacted]

SS
MAP

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET//NOFORN~~

QUESTIONS?

~~SECRET//NOFORN~~

~~SECRET~~

ACLURM043051

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b7E

SECRET//NOFORN

(U) FBI Counterintelligence Mission

• (U) FBI is lead CI agency in the U.S. (E.O. 12333)

SECRET//NOFORN

(S) ~~SECRET//NOFORN~~

(U) What is [redacted]

▪ (U) [redacted]
Program that provides for Agents to perform the
tasks to:
- Conduct CI Investigations
- [redacted]
- Show the way (Covertly)

(S) [redacted]

(S) ~~SECRET//NOFORN~~

(U) Why We need [redacted]
(Part I [redacted])

(S) (U) Threat is real, significant, aggressive

[redacted]

~~SECRET//NOFORN~~

(S)

SECRET//NOFORN

(U) Why we need [redacted]
(Part II – The History)

(S)

(S)

- (U) 1999-2000 [redacted]
- (U) 2001: DoD Bel [redacted] Report
- (FOUO) Aug 2003 [redacted] program Established
German [redacted] (S)
- (FOUO) Jun 2003 [redacted] program Expanded
Additions [redacted] (S)
Pl [redacted] (S)
- (U) 2004: Decant [redacted] buildout
- (U) 2006 [redacted] Program Mature
- (U) 2008: Long Term Planning

SECRET//NOFORN

(S)

~~SECRET//NOFORN~~

(U) ☐ Assignment - Desired
Minimum Qualifications

- (U) Five years investigative experience
- (U) Emphasis on FCI
- (U) Strong technical background
- (U) Effective leadership, interpersonal, and liaison skills
- (U) Ability to act independently with another federal agency
- (U) Can represent the FBI well

~~SECRET//NOFORN~~

b1
b7E

A diagram of a rectangle. A dashed line labeled (S) is drawn parallel to the top edge. There are two tick marks on the top edge and two tick marks on the bottom edge.

(S)

~~SECRET~~

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

7

(S)

~~SECRET//NOFORN~~

(U) [redacted]

- (FOUO) [redacted] Special Agents assigned
- [redacted] Full-time
- [redacted] Part-time
- (U) [redacted] locations
- (U) On Site Facilities (or in buildout)

[redacted]

~~SECRET//NOFORN~~

b1
b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

(S)

~~SECRET//NOFORN~~

A Day in the Life of an
Special Agent

- (U) Investigations – all varieties including 65 matters
- (U) Liaison

(S)

(FOUO) Daily Challenges

- American/scientific community openness
- egos & personalities
- Balancing additional requirements of field office

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

(U) Working with [redacted] Labs

- Contact the local [redacted] (U) of [redacted] [redacted]
- [redacted] has excellent working relationships
- Work with [redacted] to get access to [redacted] employees
- No front coordination is the name of the game with [redacted]
- [redacted]: Likely not FBI/LE
- Friendly; borderline hostile/non-cooperative
- NR is likely there as well so factor them in

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

(U) [redacted]

[redacted]

~~SECRET//NOFORN~~

b1
b7E

(S)

~~SECRET//NOFORN~~

(U) Case Examples

[redacted]

Neutralization

Espionage

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) Prominence with Decision Makers

"We have focused on working with those who may be targets of foreign counterintelligence efforts... We implemented an "Agents in the Lab" program in specific DOE facilities for the purpose of raising counterintelligence awareness and broadening the FBI's access to intelligence within the labs."

- Robert S. Mueller III
FBI Director

Written Statement before House Appropriations Subcommittee on Science, the Departments of State, Justice and Commerce, and Related Agencies, September 14, 2006.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

QUESTIONS?

~~SECRET//NOFORN~~

b1
b6
b7C
b7E

~~SECRET~~

~~SECRET~~

DATE: 02-17-2012
CLASSIFIED BY 65179/DMH/BAW/STP/stw
REASON: 1.4 (c)
DECLASSIFY ON: 02-17-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b7E

(S)

~~SECRET//NOFORN~~

FBI Counterintelligence
Division

[Redacted]

Program Managed by [Redacted]

The overall classification of this briefing is ~~SECRET//NOFORN~~

Unmarked bullets are UNCLASSIFIED

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

The Situation

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

The Situation:

[Redacted]

*We have what they want...
...and they know it...
...because we collaborate with them...
...and welcome them with open arms*

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

The Situation:

[Redacted]

Any US concerns here?

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

[Redacted]

[Redacted]

~~SECRET//NOFORN~~

b1
b7E

(S)

(S)

(S)

(S)

b1
b7E

(S)

~~SECRET//NOFORN~~

Cont'd)

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

- Protect our sensitive national resources
- Stop illegal acquisition of protected technology by foreign powers which could harm national security

[Redacted]

~~SECRET//NOFORN~~

(S)

~~SECRET//NOFORN~~

[Redacted]

[Redacted]

[Redacted]

~~SECRET//NOFORN~~

~~SECRET~~

~~SECRET~~

ACLURM043054

FBI041954

~~SECRET~~

~~SECRET//NOFORN~~

(S)

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

Foundation & Timeline

- 1999-2000 [Redacted]
- 2001: DOJ [Redacted] Report
- Aug 2003 [Redacted] Program Established
- Perm [Redacted] (SAs)
- Jun 2004 [Redacted] Program Expanded
- Additl onal [Redacted] (SAs)
- PIU [Redacted] (SAs)
- 2004-Pre [Redacted] Build-out
- 2006-Pre [Redacted] Program Mature

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

Deployment

- (FOUO) [Redacted] Special Agents assigned
- [Redacted] Full time
- [Redacted] Part-time
- [Redacted] locations
- On-Site Facilities (or in nearby RA's)

DOE CI

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

(S)

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

[Redacted]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

Agent Duties

- Investigations - all varieties including GS matters
- [Redacted]

Daily Challenges

- American/scientific community openness
- [Redacted] Culture: Science vs. Security
- [Redacted] 190's personalities
- Balancing additional requirements of field office

~~SECRET//NOFORN~~

b1
b7E

~~SECRET//NOFORN~~

(S)

Assignees:

Desired Qualifications

- Five years investigative experience
- Emphasis on FCI; Cyber a plus
- Technical background
- Effective leadership, interpersonal, and liaison skills
- Ability to act independently with USG partner agency, and represent the FBI well

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

Operating in [Redacted] Complex

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(S)

[Redacted]

~~SECRET//NOFORN~~

~~SECRET~~

~~SECRET~~

What an FBI Agent needs to know

b1
b7E

- Sooner or later something related to [redacted] facility will cross your desk
- All FBI domains have universities/colleges that likely have engineering/sciences schools
 - US technology "out-sourced"
 - Scholars/Researchers/Visitors/Conferences
 - DOE Lab job is chance assignment
 - Scientists move around/ extensive interaction/seek peer review/foreign travel
- Another resource: CARDS, IIRs, Threat Assessments

Take Aways

- Use the

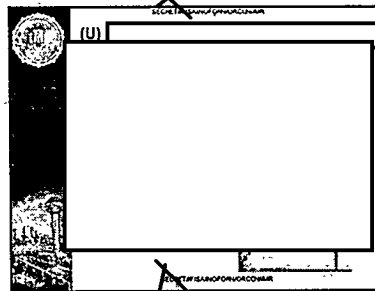
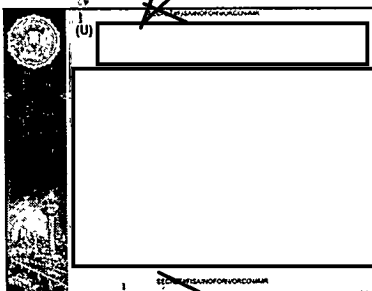
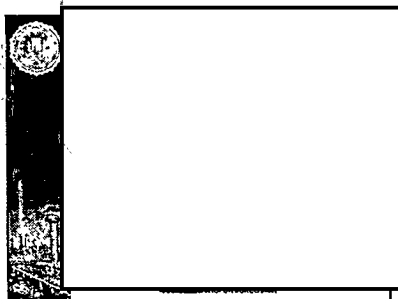
QUESTIONS?

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

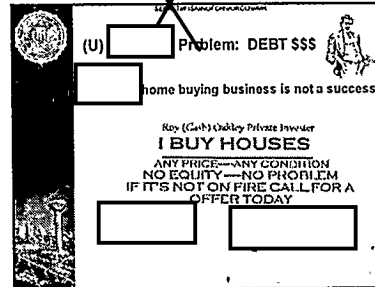
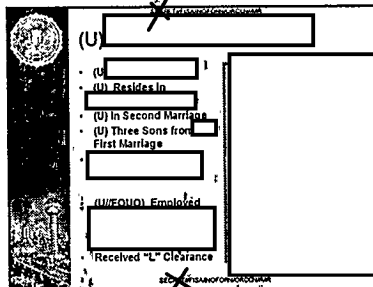
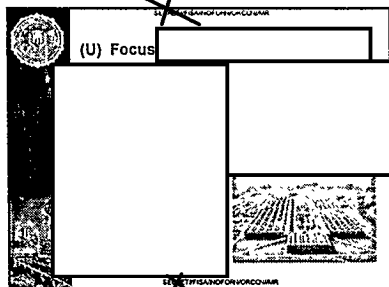
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

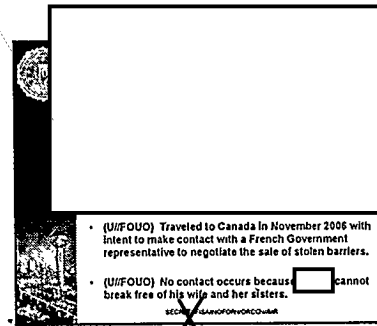
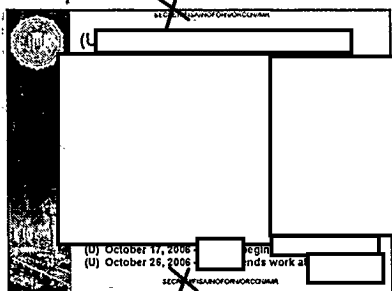


b1
b7E



b6
b7C
b7E

(S)



b1
b6
b7C
b7E

~~SECRET~~

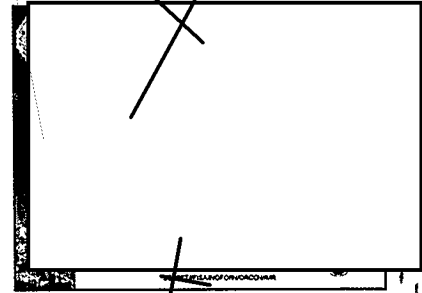
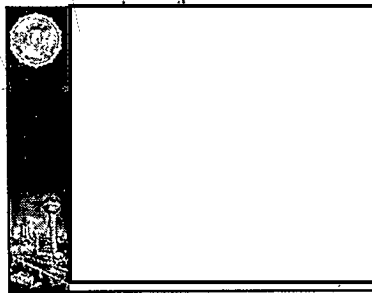
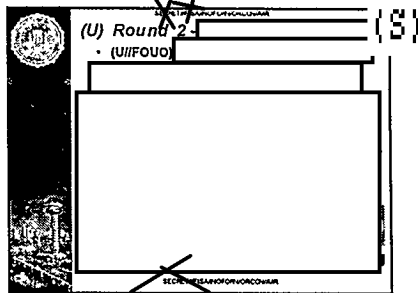
ACLURM043057

FBI041957

~~SECRET~~

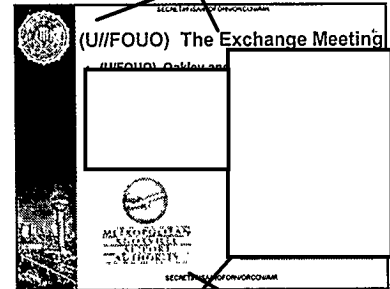
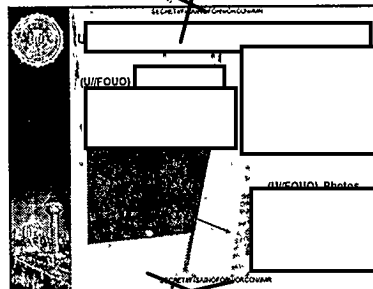
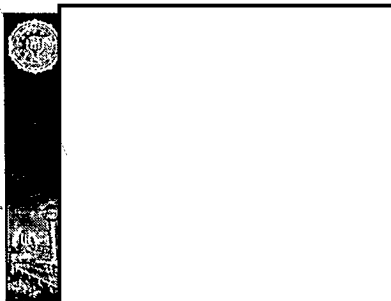
(S)

(S)

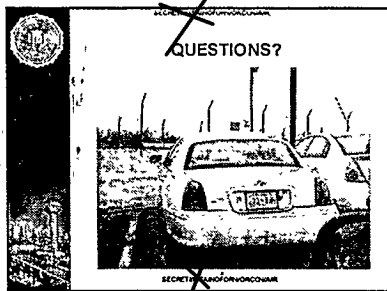


b1
b6
b7C
b7E

(S)



b1
b6
b7C
b7E



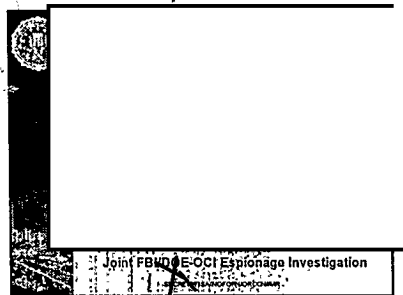
~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

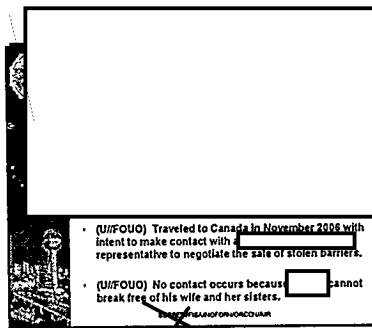
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

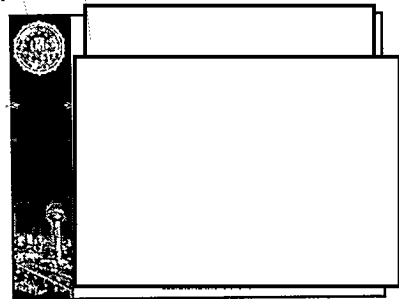
(S)



(S)

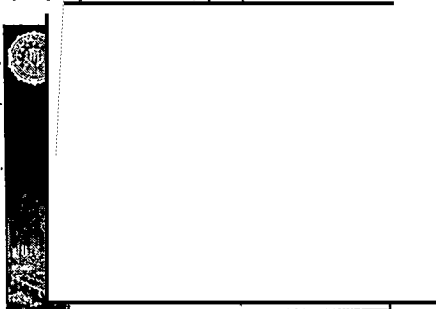


(S) (S)

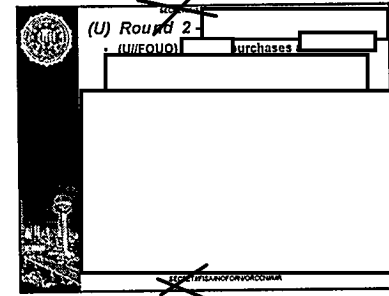
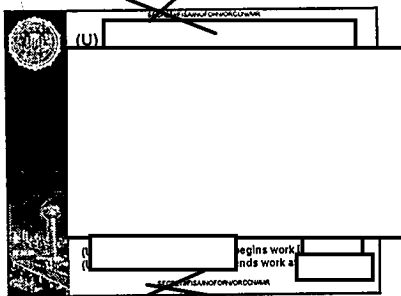


b1
b6
b7C
b7E
b7D

(S)

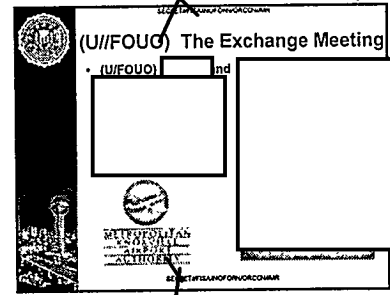
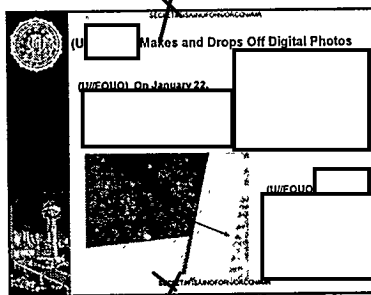
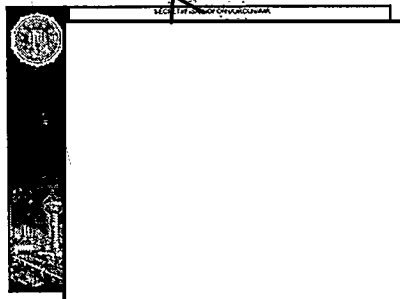


(S)



b1
b6
b7C
b7E

(S)



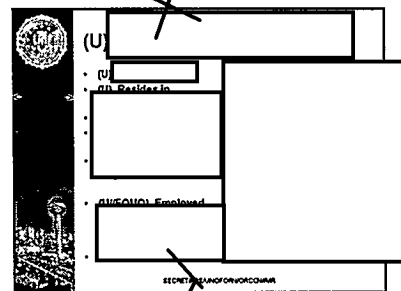
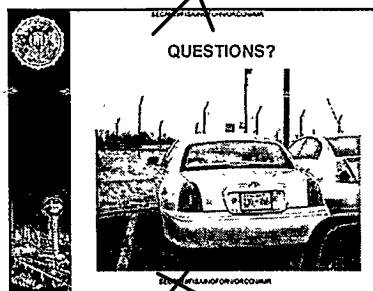
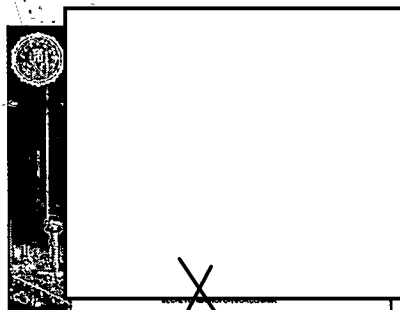
~~SECRET~~

ACLURM043059

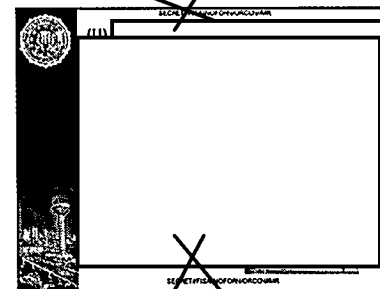
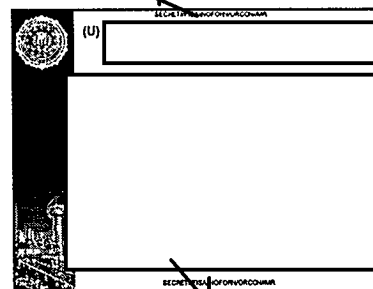
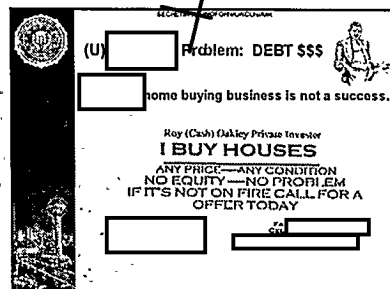
FBI041959

~~SECRET~~

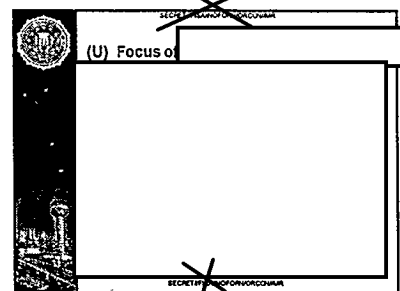
(S)



b1
b6
b7C
b7E



b6
b7C
b7E



~~SECRET~~

~~Secret/Noform~~

Investigative Toolbox: Basic Tools

CIORs

04/05/2006

DATE: 02-15-2012

CLASSIFIED BY 65179 DMH/STW

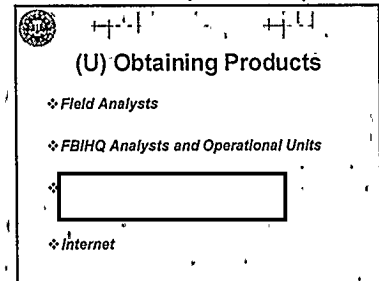
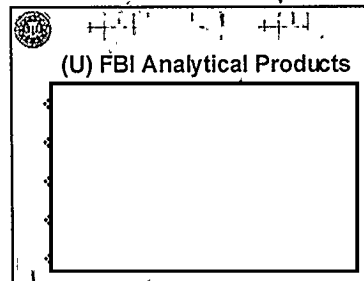
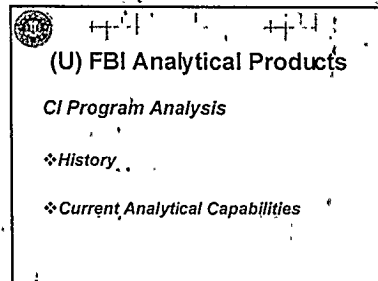
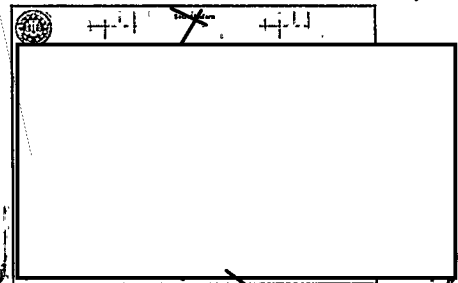
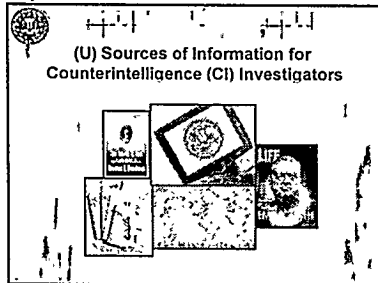
REASON: 1.4 (C)

DECLASSIFY ON: 02-15-2037

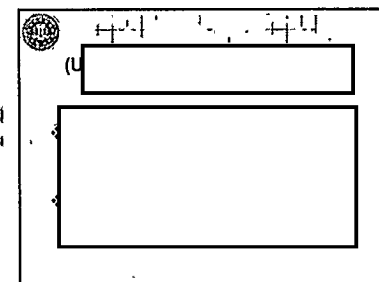
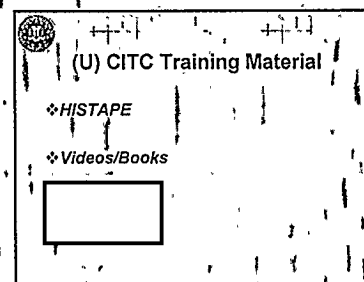
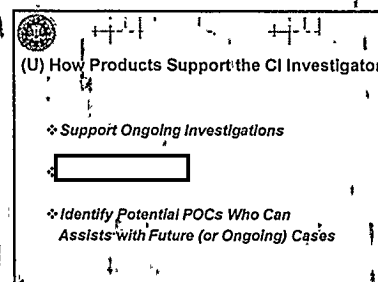
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b7E



b7E



b7E

~~SECRET~~

Updated on 04/03/2006

~~Secret/Noform~~

ACLURM043061

FBI041961

~~SECRET~~

~~Secret/Noform~~
Investigative Toolbox: Basic Tools

CIOPs
04/05/2006

(U)  Courses

- ❖ "Introduction to Counterintelligence"
- ❖ "Introduction to FISA"
- 
- ❖ "Counterintelligence Interviews"

(U) HISTAPE

- ❖ History of The FBI's FCI Program
- 
- ❖ Support Tools
- ❖ Management Issues
- ❖ Cultural/Topical Issues

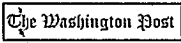
(U) CITC Videos/Books



b7E

(U) Open Source Material







(U) Books



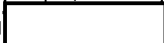



(U) Magazines, Periodicals, & Newspapers

- ❖ "Washington Post"
- ❖ "Economist"
- ❖ "Wall Street Journal"
- ❖ "US News and World Report"

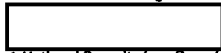
(U) Libraries

- ❖ Local Libraries
- ❖ FBI Academy Library

(U)  the Internet




(U) 

- ❖ Counterintelligence Division
- ❖ Directorate of Intelligence
- 
- ❖ National Security Law Branch
- ❖ Office of General Counsel (OGC)
- ❖ Office of International Operations (OIO)

b7E

~~SECRET~~

Updated on 04/03/2006
~~Secret/Noform~~
ACLURM043062

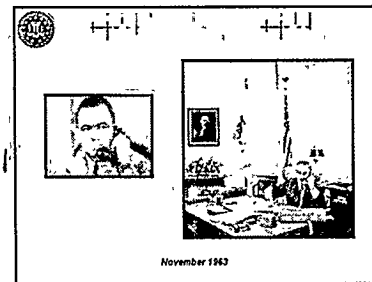
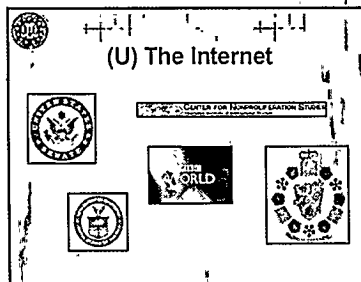
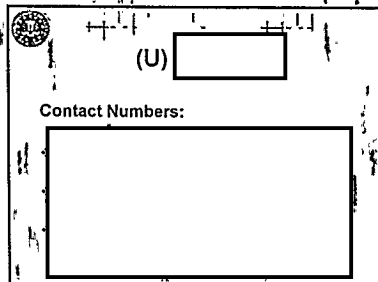
~~SECRET~~

~~Secret/Noform~~

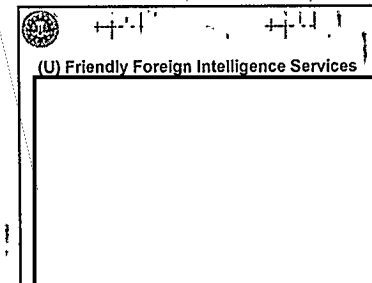
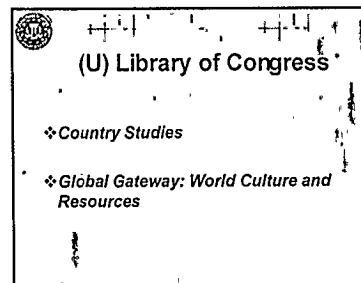
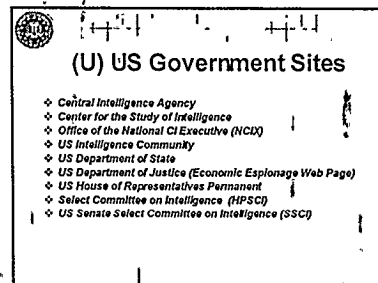
Investigative Toolbox: Basic Tools

CIOPs

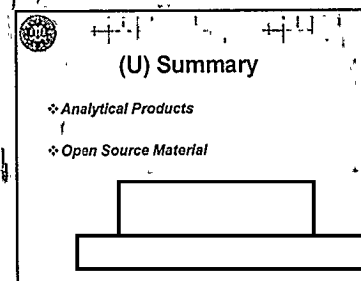
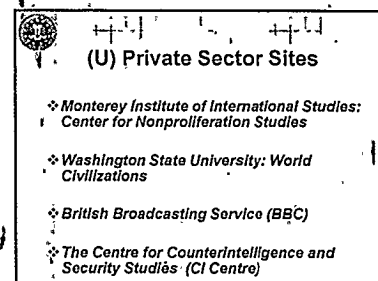
04/05/2006



b7E



b1
b7E



b6
b7C
b7E

~~SECRET~~

Updated on 04/03/2006

~~Secret/Noform~~

ACLURM043063

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

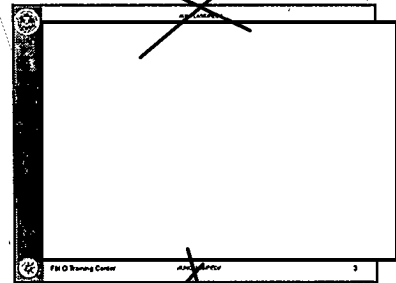
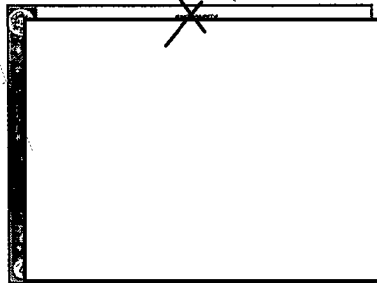
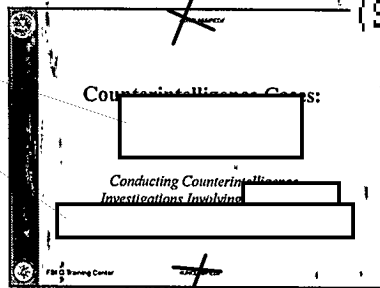
~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)

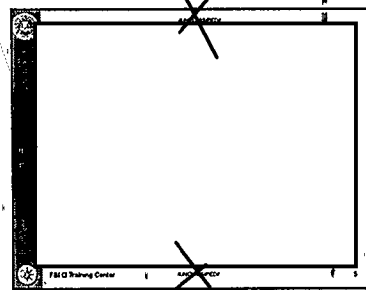
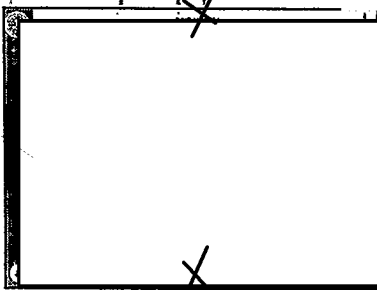
(S)



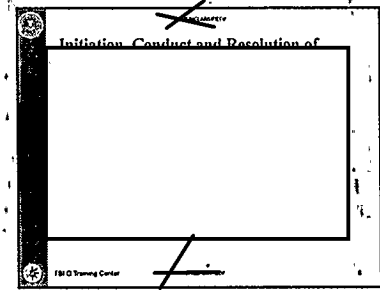
b1
b7E

(S)

(S)



(S)

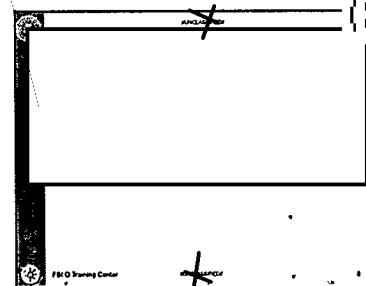
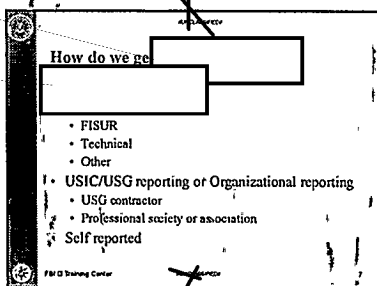


b1
b7E

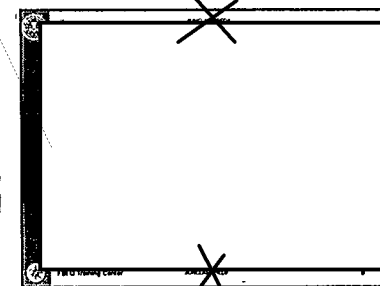
(S)

(S)

(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

b1
b7E

(S)

How do the objectives of [redacted] coincide with the FBI's CI Strategy? 09

- CI Strategic Goals
 - Preventing proliferation of WMD
 - Preventing penetration of the USIC
 - Preventing penetration of USG and contractors
 - Prevent compromise of CNAs

FBI Q Training Center [redacted] 10

(S)

How do the objectives of [redacted] coincide with the FBI's CI Strategy? 09

- CI Strategic Goals
 - Identify [redacted]
 - Disrupt the [redacted]
 - Change behavior of [redacted]

FBI Q Training Center [redacted] 11

(S)

How do the objectives of [redacted] coincide with the FBI's CI Strategy? 09

- CI Program Strategies
 - Know the domain
 - Understand the threat
 - Conduct sophisticated operations
 - Create and maintain strategic partnerships
 - Inform and influence Policymakers

FBI Q Training Center [redacted] 12

(S)

Evaluating and prioritizing [redacted] 09

- Role of the SSA
 - Volume precludes opening every case
 - Evaluate information received in perspective of national CI Program Strategy goals
 - Assess case workload on squad
 - O & A cases which appear relevant

FBI Q Training Center [redacted] 13

(S)

Evaluating and prioritizing [redacted] 09

- Responsibility of the Case Agent
 - Know the CI Program Strategy
 - Assess cases regularly
 - Obtain comprehensive background on both subjects
 - Thoroughly research Main Subject's country
 - Maintain working AND interactive liaison

FBI Q Training Center [redacted] 14

(S)

Elements of [redacted] investigative [redacted]

- Post-Interview Evaluation
 - Evaluating results of interview and other investigative findings

FBI Q Training Center [redacted] 15

b1
b7E

(S)

Preparation [redacted]

- Specific checks on [redacted] Subject
 - FBI
 - USIC
 - State & local
 - Military
 - Clearances
 - Open source
 - Others as indicated

FBI Q Training Center [redacted] 16

(S)

Preparation [redacted]

- Conduct records checks / file reviews on [redacted] Subject
 - Employment
 - Current
 - Prior
 - Professional affiliations
 - "Off duty" interests and/or activities
 - Immediate family
 - Ethnic & other background

FBI Q Training Center [redacted] 17

(S)

Preparation [redacted]

- Conduct records checks / file reviews on Main Subject
 - Status
 - Assigned in your turf
 - TDY to your turf
 - Intelligence affiliation
 - Job function and responsibilities
 - "Off duty" interests and habits

FBI Q Training Center [redacted] 18

~~SECRET~~

~~SECRET~~

(S)

(S)

Elements of an [redacted] investigative plan

FBI Training Center [redacted]

(S)

(S)

Elements of an [redacted] interview plan

- Establishing need & requirement to interview
- Based on access [redacted]
- Considerations for interview [redacted]
- Potential of advising Main Subject or Media

FBI Training Center [redacted]

(S)

Execution

- Approach [redacted]
- Location & Time
- Explain why interview is necessary
- Direct or Pretend
- Protect sources

FBI Training Center [redacted]

b1
b7E

(S)

(S)

Execution

Questions

- About the [redacted] Subject

[redacted]

- Description & discussion
- Desire to develop personal relationship

FBI Training Center [redacted]

(S)

Execution

- Questions
- About the Main Subject

[redacted]

FBI Training Center [redacted]

Problems during the interview

- Denials, inconsistencies...
- Keep the door open and come back
- Not cooperative/hostile
- Legitimate concerns about talking to the FBI - family, employment, etc.

FBI Training Center [redacted]

b1
b7E

(S)

[redacted]

- Because there may be
- Unresolved issues or conflicts
- Additional questions
- About topics discussed
- About topics not discussed
- Need to further assess asset potential

FBI Training Center [redacted]

(S)

(S)

(S)

Post-interview evaluation

- Have you [redacted]
- Obtained new or corroborative info on the Main Subject
- Adequately assessed the [redacted] object's asset potential

[redacted]

FBI Training Center [redacted]

(S)

[redacted]

- Follow up questions
- Rephrase some questions from first interview
- Elicit additional information concerning the Main Subject
- Elicit additional background information concerning the [redacted] object
- Address any conflicting or inconsistent issues

FBI Training Center [redacted]

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

(S)

Evaluating the results of the interview and other investigative findings

Subject

Is Main Subject

Have all matters been resolved?

FBI Q Training Center

(S)

(S)

(S)

(S)

Follow-up options

Main Subject

Criminal potential again

d/or Main

FBI Q Training Center

Exercise 1

The Professor and The Scientist

FBI Q Training Center

b1
b7E

(S)

(S)

SUMMARY:

Definition

Goal

Objectives

Connection to National CI Strategy

FBI Q Training Center

b1
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

~~Counterintelligence Cases~~

(S)

~~Conducting Counterintelligence
Investigations Involving~~

FBI Training Center

(S)

(S)

(S)

- What categories are included?
- Tourists
 - Business people
 - Scholars
 - Cultural, sports, scientific and others
 - Government & non-government sponsored
 - Individuals and delegations

FBI Training Center

b1
b7E

(S)

(S)

FBI Training Center

(S)

FBI Training Center

(S)

People
Places
Things
Information

FBI Training Center

(S)

(S)

(S)

(S)

(S)

Potential far-reaching consequences

FBI Training Center

(S)

~~Do your research~~

- Domain
- Host
- Liaison
- USIC/USG
- Business / Academia
- Sponsoring organizations

FBI Training Center

(S)

Sources

- Professional
- Private

Possible techniques

- Mail and/or mesh covers

Interview of [] and host/sponsor

FBI Training Center

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

(S)

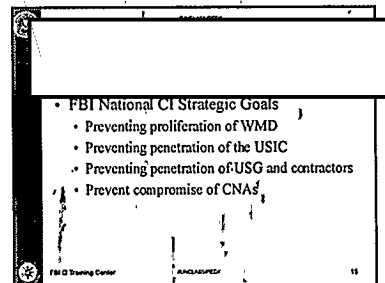
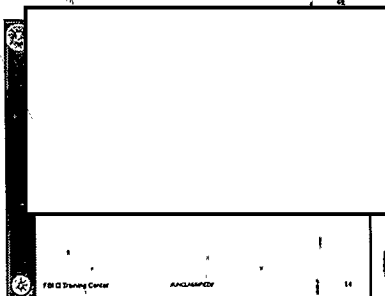
(S)

b1
b7E

(S)

(S)

(S)



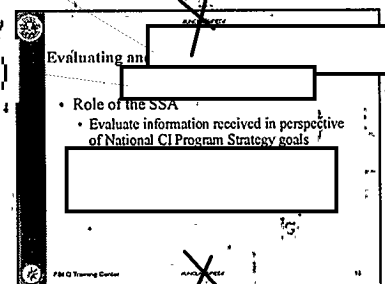
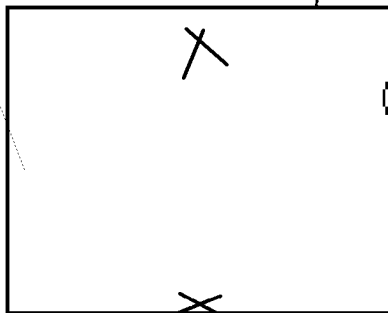
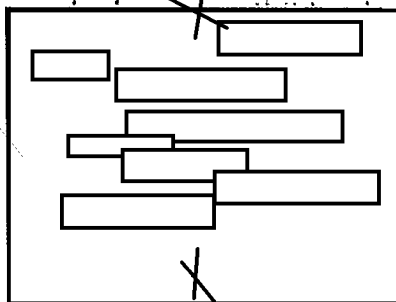
b1
b7E

(S)

(S)

(S)

(S)



b6
b7C
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

(S)

Evaluating and [redacted]

- Responsibility of the Case Agent
- Know the CI Program Strategy

[redacted]

FBI Training Center [redacted] 19

(S)

[redacted] Exercise #2

[redacted]

FBI Training Center [redacted] 20

(S)

Elements of [redacted]

[redacted]

- Evaluation of interview results & investigative findings

FBI Training Center [redacted] 21

(S)

(S)

(S)

b1
b7E

(S)

Elements of [redacted]

- Records checks

[redacted]

- Re-checks

FBI Training Center [redacted] 22

(S)

(S)

Elements of a [redacted]

[redacted]

FBI Training Center [redacted] 23

(S)

Elements of a [redacted]

- Preparation
- Execution

[redacted]

- Post-interview Evaluation

FBI Training Center [redacted] 24

(S)

(S)

(S)

b1
b7E

(S)

(S)

Elements of [redacted]

- Determine need/commitment to interview

[redacted]

- Considerations for interview
 - Subject isn't cooperative or is hostile
 - Diplomatic protest
 - Negative publicity

FBI Training Center [redacted] 25

(S)

Elements of [redacted]

- The Approach
 - Initial Contact
 - Going it alone
 - Direct or pretext?
 - Location
 - Cultural concerns and issues

FBI Training Center [redacted] 26

(S)

Elements of a [redacted]

- Questions
 - Theirs
 - Yours
- Problems during interview
 - Denials/inconsistencies
 - Challenge

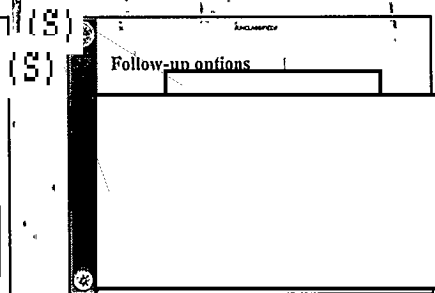
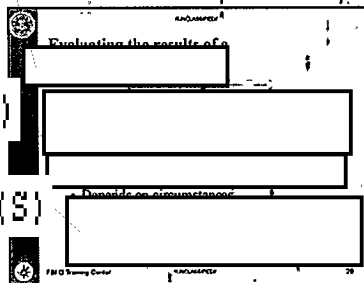
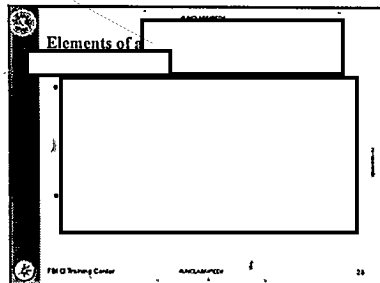
FBI Training Center [redacted] 27

~~SECRET~~

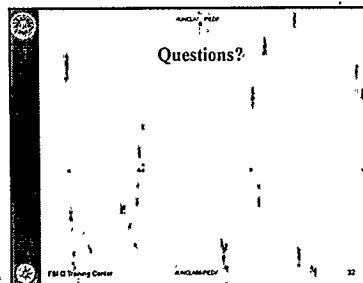
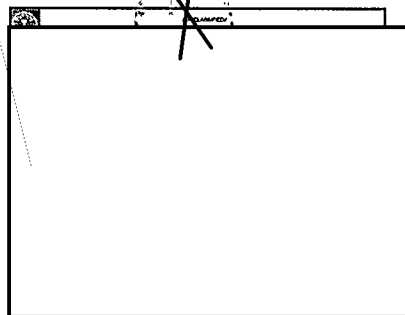
~~SECRET~~

(S)

(S)



(S)

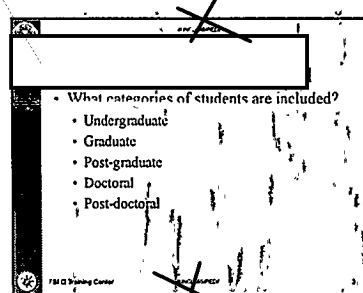
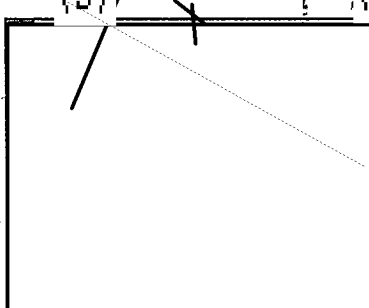
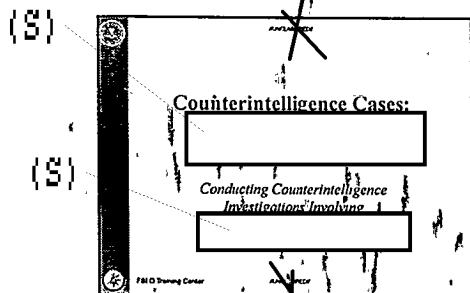


b1
b7E

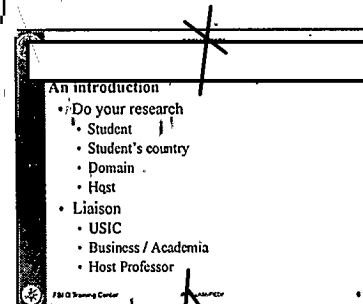
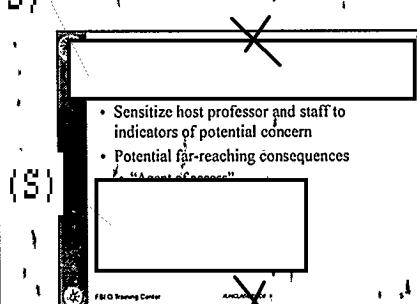
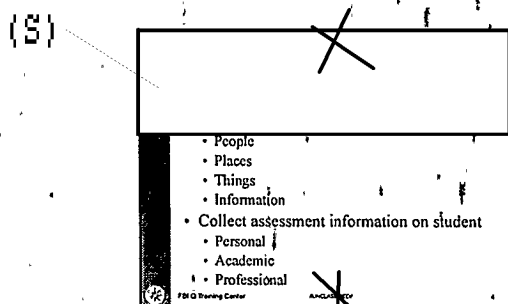
~~SECRET~~

~~SECRET~~

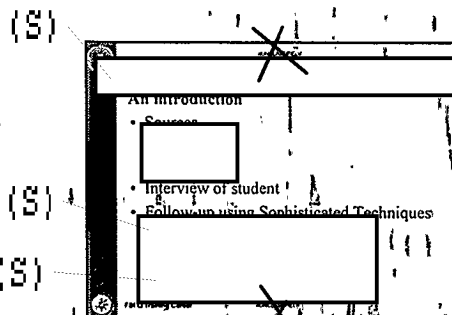
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



b1
b7E



b1
b7E



b1
b7E

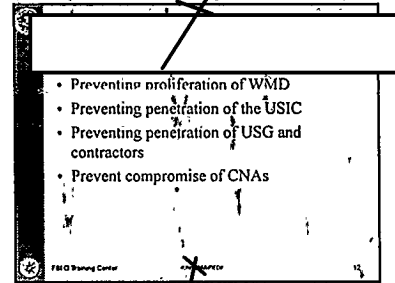
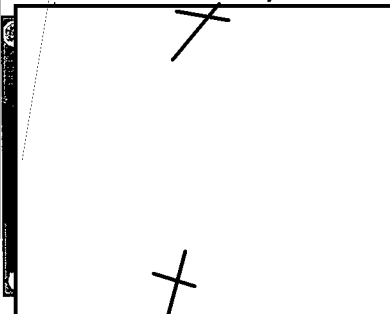
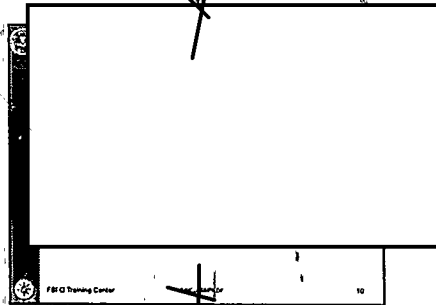
~~SECRET~~

~~SECRET~~

(S)

(S)

(S)



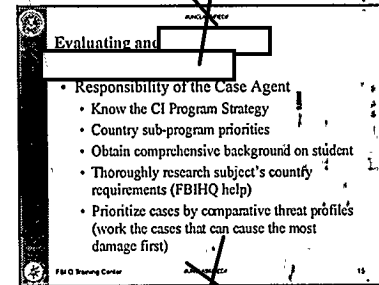
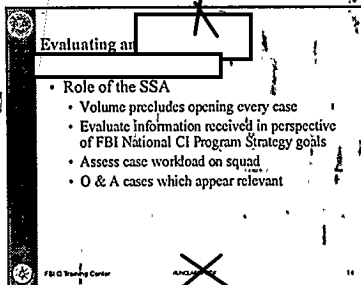
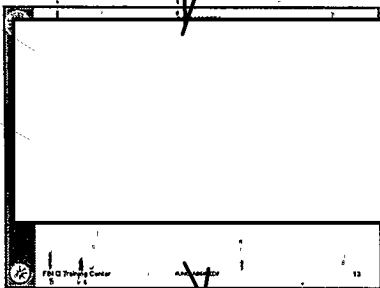
b1
b7E

(S)

(S)

(S)

(S)



b1
b7E

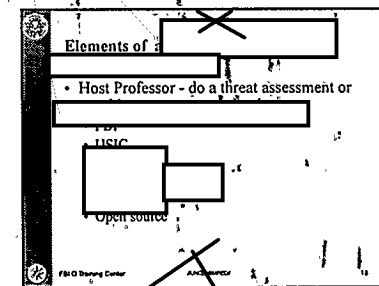
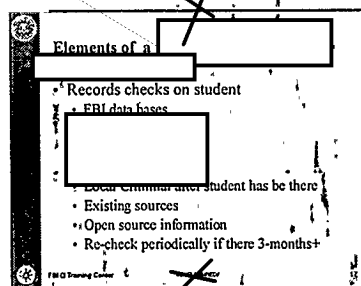
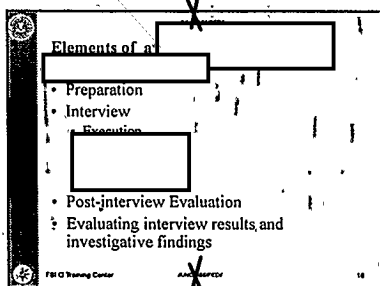
(S)

(S)

(S)

(S)

b1
b7E



~~SECRET~~

~~SECRET~~

(S)

Elements of a [redacted]

[redacted]

[redacted]

FBI Training Center [redacted] 19

(S)

Elements of a [redacted]

- When student there for more than 3-months
- Student cases are not snapshots
 - Circumstances can change
 - Be prepared to go back if warranted

FBI Training Center [redacted] 20

(S)

Elements of a [redacted]

- Denomination
- Execution
- Post-interview Evaluation

FBI Training Center [redacted] 21

b1
b7E

(S)

Elements of a [redacted]

- Determine need / requirement to interview

[redacted]

FBI Training Center [redacted] 22

(S)

Elements of a [redacted]

- The Approach
 - Direct or pre-emptive
 - Location
 - Cultural concerns and issues

FBI Training Center [redacted] 23

(S)

Elements of a [redacted]

- Execution
 - Questions
 - Theirs
 - Yours
 - Recontact by USG*
 - Problems during interview
 - Benign
 - "Active"

FBI Training Center [redacted] 24

(S)

Elements of a [redacted]

- Post-interview evaluation
 - A better idea of the threat?
 - Can you make a call on asset potential?
- Recontact & follow up questions
 - Rephrase some questions from first interview

FBI Training Center [redacted] 25

(S)

Elements of a [redacted]

- Is there a threat to U.S. national security?
- Is the student [redacted] or [redacted] willing to cooperate?
- Does length of stay require [redacted]

FBI Training Center [redacted] 26

(S)

Follow-up options

[redacted]

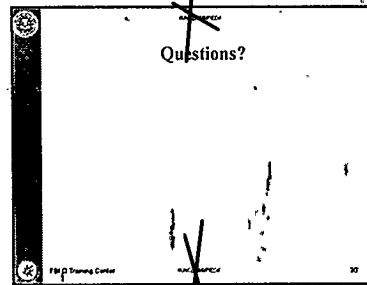
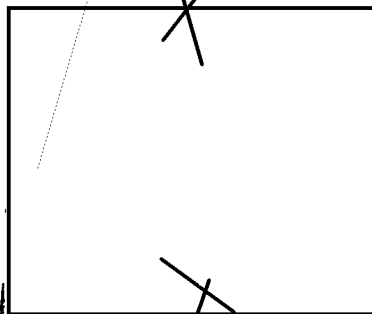
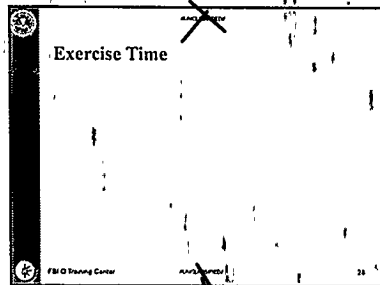
FBI Training Center [redacted] 27

b1
b7E

~~SECRET~~

~~SECRET~~

(S)



b1
b7E

~~SECRET~~

DATE: 02-15-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-15-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)

Counterintelligence Cases:

Conducting Counterintelligence

FBI Training Center

(S)

FBI Training Center

(S)

What is a [redacted]

What categories of [redacted] are included?

- Tourists
- Business people
- Students, scholars, or professors
- Cultural, sports, scientific and others
- Government & non-government sponsored
- Individuals and delegations

FBI Training Center

b1
b7E

(S)

(S)

(S)

FBI Training Center

(S)

FBI Training Center

(S)

(S)

What is a [redacted]

- People
- Places
- Things
- Information

FBI Training Center

b1
b7E

(S)

(S)

Sensitize host/sponsor (if any) to indicators of potential concern

Potential far-reaching consequences

FBI Training Center

(S)

Do your research

- Subject
- Subject's country
- Domain
- Host
- Liaison
- USIC/USG
- Business / Academia
- Sponsoring organizations

FBI Training Center

(S)

(S)

(S)

Sources

- Private
- Possible techniques
- Mail and/or transit covers
- Interview host/sponsor

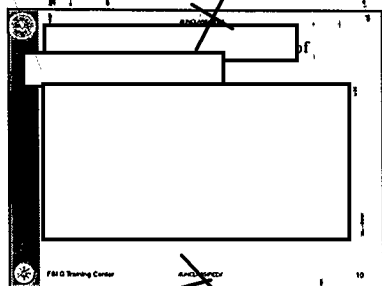
FBI Training Center

b1
b7E

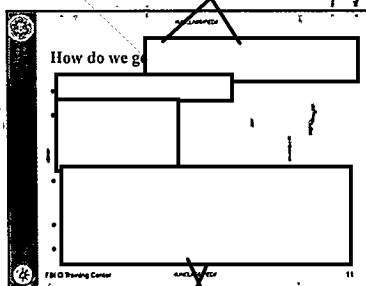
~~SECRET~~

~~SECRET~~

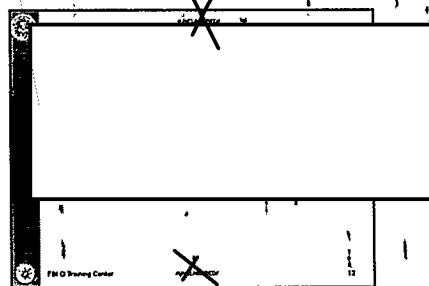
(S)



(S)



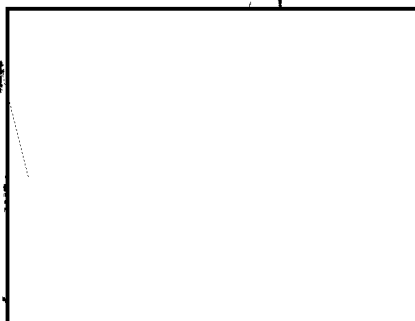
(S)



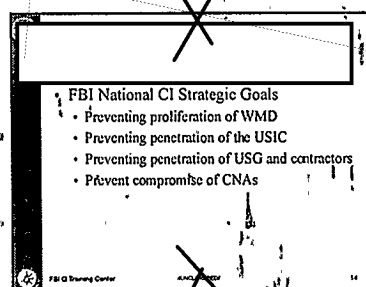
b1
b7E

(S)

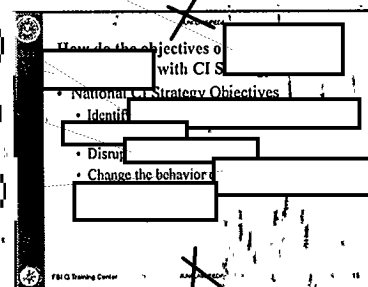
(S)



(S)



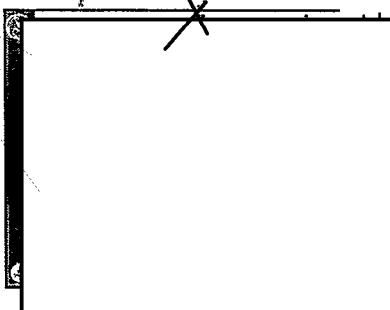
(S)



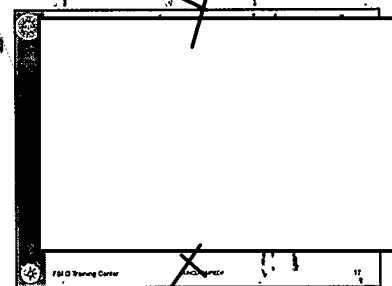
b1
b7E

(S)

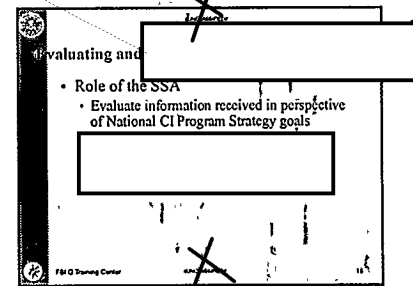
(S)



(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

(S)

~~Evaluating and~~

- Responsibility of the Case Agent
- Know the CI Program Strategy
- Count
- Threat profile of each case

FBI Training Center

(S)

~~Elements of~~

investigative strategy

- Preparation
- Interview Execution
- Evaluation of interview results & investigative findings

FBI Training Center

(S)

~~Elements of a foreign~~

investigative strategy

Records checks

- Available open source information
- Re-checks

FBI Training Center

b1
b7E

(S)

~~Elements of a~~

investigative strategy

FBI Training Center

(S)

~~Elements of~~

- Preparation
- Execution
- Post-interview evaluation

FBI Training Center

(S)

~~Elements of a~~

interview plan

Determine need/requirement to interview

FBI Training Center

b1
b7E

(S)

~~Elements of a~~

The Approach

- Disrupt or pretext?
- Location
- Cultural concerns and issues

FBI Training Center

(S)

~~Elements of a~~

- Questions
 - Theirs
 - Yours
- Problems during interview
 - Denials/inconsistencies
 - Challenge

FBI Training Center

(S)

~~Elements of a~~

- Post-interview evaluation
 - Information obtained
 - Attitude and demeanor of subject
 - Corroboration of existing information
 - Analysis
- Follow up questions
 - Rephrase some questions from first interview

FBI Training Center

b1
b7E

~~SECRET~~

~~SECRET~~

(S)

(S)

(S)

~~SECRET~~

Evaluating the results of

- Is there a threat to U.S.

FBI Training Center

(S)

(S)

(S)

~~SECRET~~

Follow-up options

FBI Training Center

~~SECRET~~

Exercise #2

FBI Training Center

b1
b7E

(S)

(S)

(S)

~~SECRET~~

Summary

Conclusion

FBI Training Center

~~SECRET~~

Questions?

FBI Training Center

~~SECRET~~

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

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

(S)

Counterintelligence Cases

Conducting Counterintelligence Investigations

FBI CI Training Center

(S)

FBI CI Training Center

(S)

What categories of [redacted] are include d?

- Tourists
- Business people
- Students and scholars
- Cultural, sports, scientific and others
- Government & non-government sponsored
- Individuals and delegations

FBI CI Training Center

b1
b7E

(S)

FBI CI Training Center

(S)

FBI CI Training Center

(S)

People

Places

Things

Information

FBI CI Training Center

b1
b7E

(S)

Potential far-reaching consequences

FBI CI Training Center

(S)

Do your research

- Host
- Liaison
- USCUSG
- Business / Academia
- Sponsoring organizations

FBI CI Training Center

(S)

Professional

Private

Possible techniques

Mail and/or trash covers

Interview [redacted] and host/sponsor

FBI CI Training Center

b1
b7E

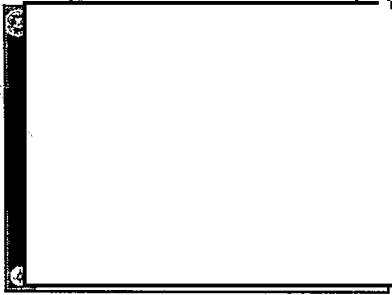
~~SECRET~~

ACLURM043080

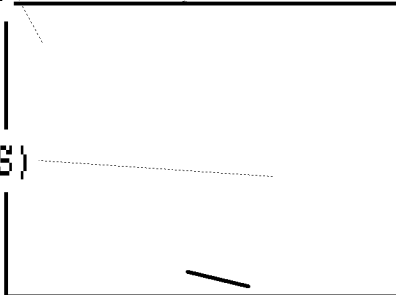
FBI041980

~~SECRET~~

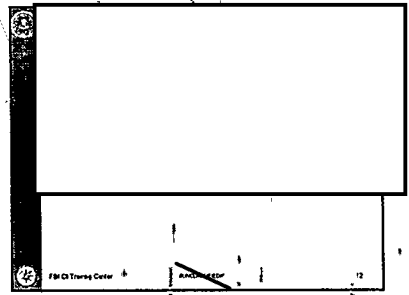
(S)



(S)

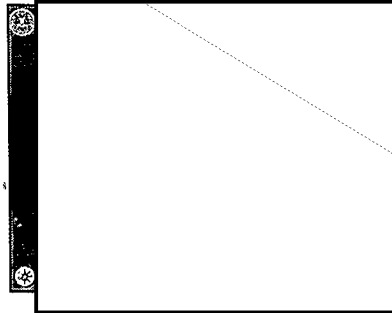


(S)

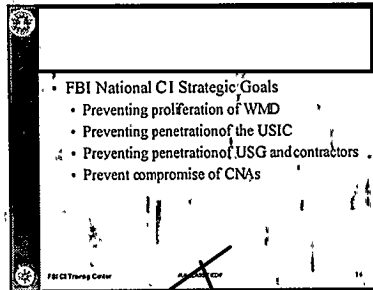


b1
b7E

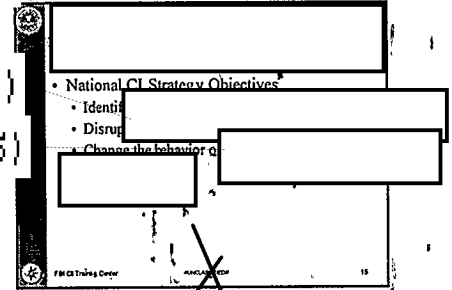
(S)



(S)



(S)



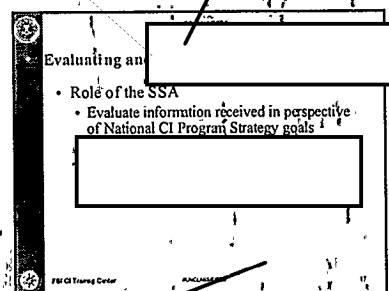
(S)

(S)

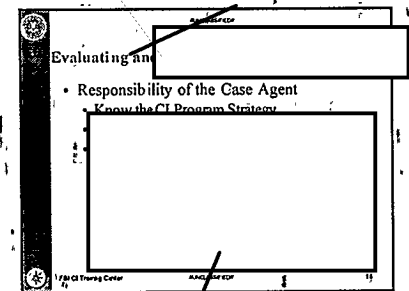
(S)



(S)



(S)

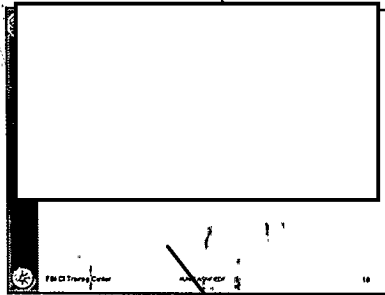


b1
b7E

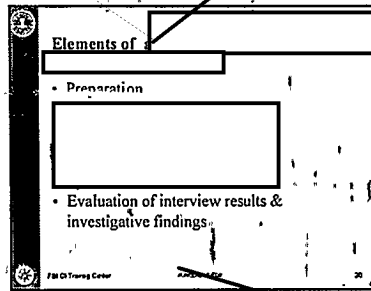
~~SECRET~~

~~SECRET~~

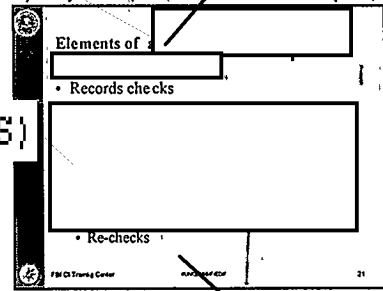
(S)



(S)

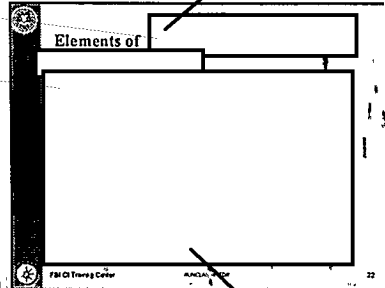


(S)

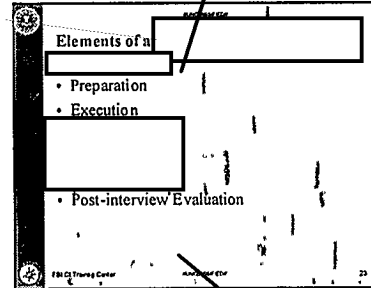


b1
b7E

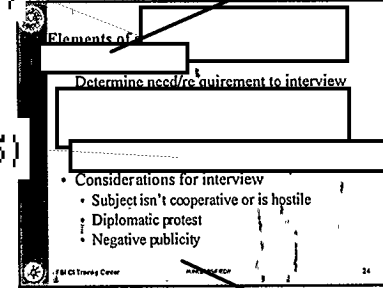
(S)



(S)

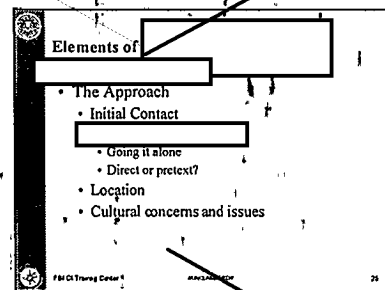


(S)

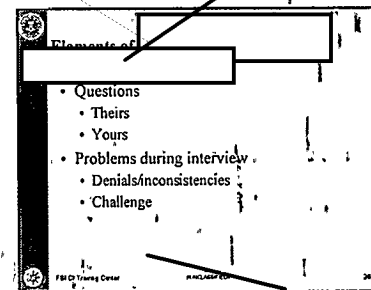


b1
b7E

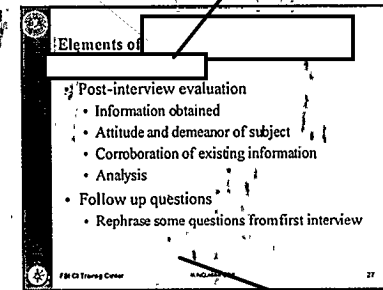
(S)



(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

(S)

What makes [redacted] different?

- Historically there has been a higher potential for misunderstanding and opposition at academic institutions
- Academic freedom issue
- Host/sponsor is a professor
- Security Officer rarely involved

FBI CI Training Center

(S)

[redacted] exercise

FBI CI Training Center

(S)

(S)

[redacted]

b1
b7E

(S)

Follow-up options

[redacted]

FBI CI Training Center

(S)

[redacted]

FBI CI Training Center

Questions?

FBI CI Training Center

b1
b7E

~~SECRET~~

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

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Counterintelligence Cases: CI Interviewing

*Planning and Conducting
Counterintelligence Interviews*

What is a CI interview?

Definition

A planned and structured conversation with an individual designed to gather information so evidence can be collected or intelligence elicited that can be used to structure or further an investigation.

How do they differ from Criminal interviews?

- No crime is known to have occurred
- Interviewees cannot be compelled to talk to the FBI
- Category of person interviewed is generally different from persons involved in routine matters

What is a successful CI interview?

- It accomplishes CI interview objectives
- The interviewee is willing to be recontacted

Why are CI interviews conducted? CI Interview Objectives

[Redacted]

[Redacted]

Why are CI interviews conducted?

- [Redacted]
- Determine if the person being interviewed has asset potential for either the FBI or the USIC

b1
b7E

Why are CI interviews conducted?

- Potential for far-reaching consequences -
- [Redacted]

CI Interview Planning

- Planning is a detailed method formulated beforehand for doing something

Elements of a CI Interview Plan

- Preparation
 - Execution
 - Post-Interview Evaluation
- [Redacted]

b1
b7E

~~SECRET~~

ACLURM043084

FBI041984

~~SECRET~~

Preparation

- Doing those things that will make you ready to conduct a CI interview
- Conduct Research on the
 - Predication of the interview
 - Investigative area of interest
- Subject

FBI Training Center

10

The Subject

- Language
- Ethnic and cultural considerations
 - Names
 - Gender
 - Habits
 - Physical issues
 - Dietary customs and rules
 - Religious matters
 - Occupation
- Is approval needed to interview?

FBI Training Center

11

Preparation – Sources for background information on Subject

- Basic law enforcement checks
 - DMV
 - FBI indices including ELSUR
 - Criminal
 - Credit
- Public Sources
 - Lexis-Nexis
 - Internet
 - Professional publications/associations

FBI Training Center

12

b7E

Preparation – Sources for background information on Subject

- US Government

US Intelligence Community

FBI Training Center

13

Execution – How are you going to conduct the interview?

FBI Training Center

14

Execution –

FBI Training Center

15

b7E

Preparation – Initiation of CI interviews

- Who will know
 - Daily associates
 - Subordinates
 - Supervisors
 - Family
 - Neighbors
- What this is about and Why
 - Direct
 - Pretext

FBI Training Center

16

Preparation – Initiation of CI interviews

- Location – must be determined in the initial contact stage
 - Work
 - Residence
 - FBI office
 - Other

FBI Training Center

17

The Interview Questions

- Preparation requires that you think through both the
 - Questions subject is likely to ask and
 - Questions you want to ask

FBI Training Center

18

~~SECRET~~

~~SECRET~~

~~SECRET~~

The Interview Questions

- Questions – Theirs
 - Who are you?
 - What are you doing here?
 - Why does the FBI want to talk to me?
 - Have I done something wrong?
 - How do you know what you know?
 - Who knows you are talking to me?
 - What do you know that I think I should know?
 - What should I do next?

FBI Q Training Center

~~SECRET~~

The Interview Questions

- Questions – yours
 - Corroborate what you know about
 - Interviewee
 - Situation that generated the interview
 - Subjects know to interview
 - Corroboration is a test of interviewee's veracity
 - BUT do not discount faulty memory or information you have may be incorrect
 - Fill in the gaps
 - Identify and address conflicting information

FBI Q Training Center

~~SECRET~~

The Interview Questions

- Questions – Yours
 - Subject's personal background
 - Name & identifying information
 - Education
 - Military
 - Volunteer work
 - Travel
 - Family information (look for derivative access)
 - Immediate
 - Parents and other relatives & locations

FBI Q Training Center

~~SECRET~~

The Interview Questions

- Questions – Yours
 - Occupation/Employment
 - Full time/part time
 - Time on the job
 - Locations
 - Nature of work
 - Travel
 - Contacts with CI targets of interest
 - Professional contacts

FBI Q Training Center

~~SECRET~~

(S)

FBI Q Training Center

~~SECRET~~

Post-Interview Evaluation

- Have objectives been met?
 - Potential threat to national security?
- Was assessment info collected?
- Acquire tradecraft?
- Asset potential?

FBI Q Training Center

b1
b7E

~~SECRET~~

Communication

True or False?

You can identify cues indicative of interviewee's mindset

...and you display cues too!

FBI Q Training Center

~~SECRET~~

FBI Q Training Center

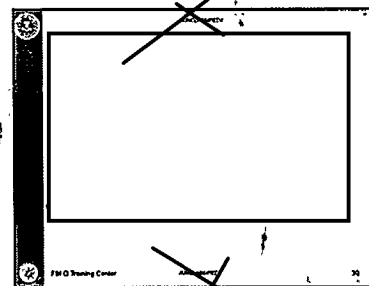
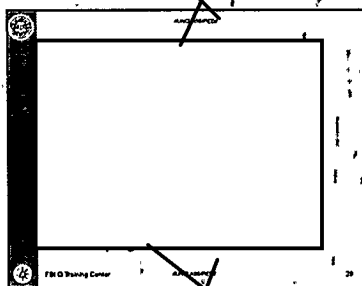
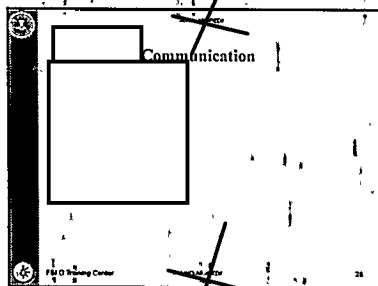
~~SECRET~~

FBI Q Training Center

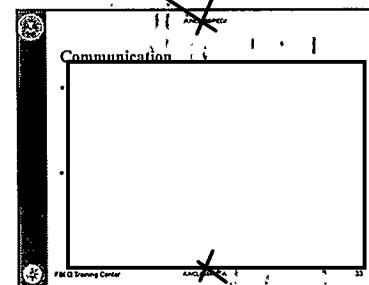
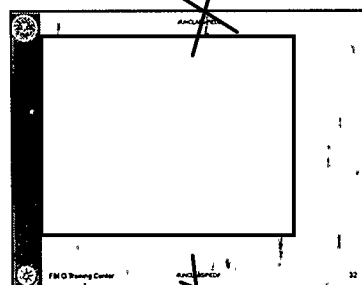
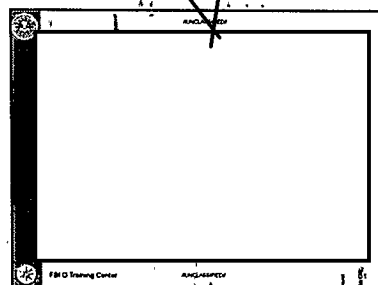
b7E

~~SECRET~~

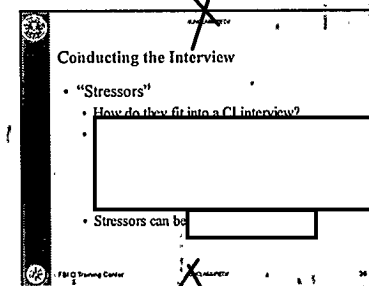
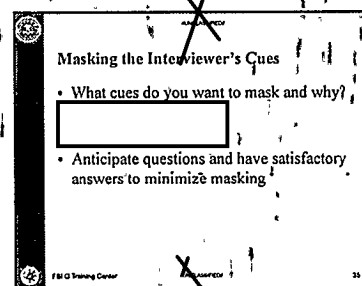
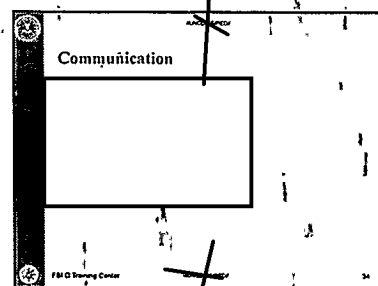
~~SECRET~~



b7E



b7E



b7E

~~SECRET~~

~~SECRET~~

~~SECRET~~

Interview Exercise

[Redacted]

FBI Training Center

~~SECRET~~

Summary

- Definition
- CI Interview is a planned and structured conversation with an individual designed to gather information, so evidence can be collected or intelligence elicited that can be used to structure of further an investigation.

(S)

FBI Training Center

~~SECRET~~

Summary

- CI Interview Objectives
- Assess potential threat to national security posed by an individual based on that person's [Redacted]
- Collect assessment information on the subject of a Preliminary or Full Investigation

FBI Training Center

b1
b7E

~~SECRET~~

Summary

- CI Interview Objectives

[Redacted]

FBI Training Center

~~SECRET~~

Summary

- Elements of a CI Interview: Plan
- Preparation
- Execution

[Redacted]

- Post-Interview Evaluation

FBI Training Center

~~SECRET~~

Questions?

FBI Training Center

b7E

~~SECRET~~

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

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

(S)

Counterintelligence Cases:

Conducting Counterintelligence Investigations Involving

FBI Training Center

(S)

(S)

What categories are included?

- Tourists
- Business people
- Scholars
- Cultural, sports, scientific and others
- Government & non-government sponsored
- Individuals and delegations

FBI Training Center

b1
b7E

(S)

(S)

(S)

People

Places

Things

Information

- Personal capabilities (access to others)
- Academic field
- Professional expertise

FBI Training Center

b1
b7E

(S)

Potential far-reaching consequences

FBI Training Center

(S)

What is your research?

- Domain
- Host
- Liaison
- USIC/USG
- Business / Academia
- Sponsoring organizations

FBI Training Center

(S)

Sources

- Professional
- Private
- Possible techniques

Interview of and host/sponsor

FBI Training Center

b1
b7E

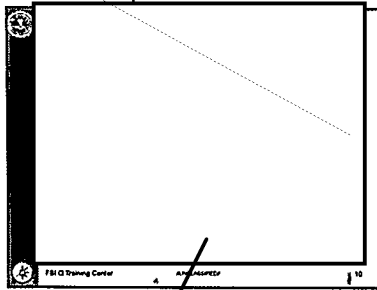
~~SECRET~~

ACLURM043089

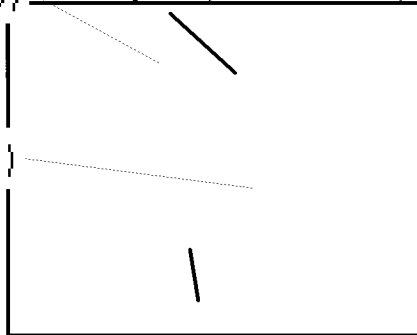
FBI041989

~~SECRET~~

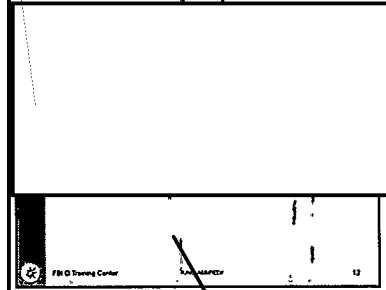
(S)



(S)



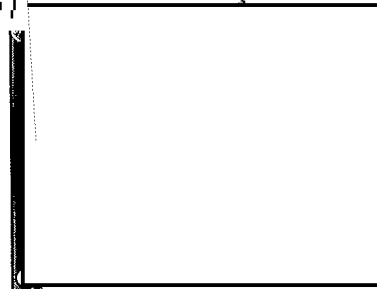
(S)



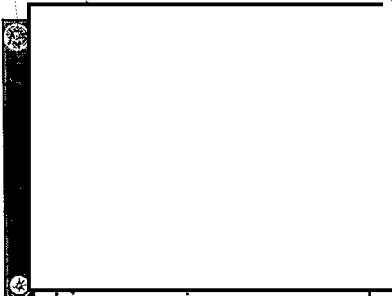
b1
b7E

(S)

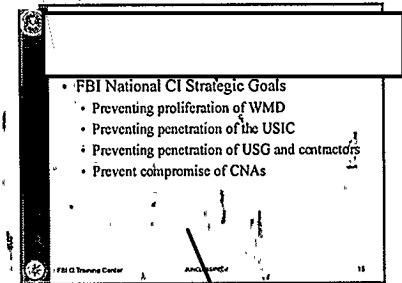
(S)



(S)



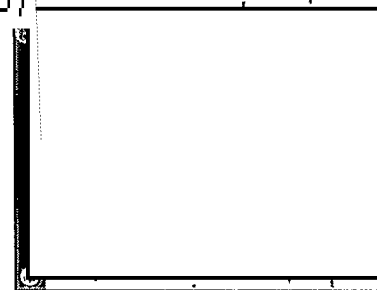
(S)



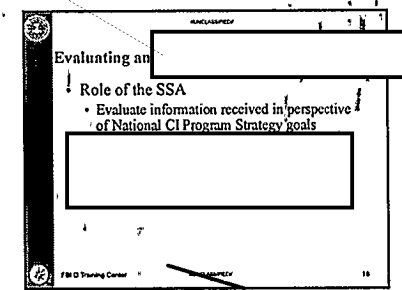
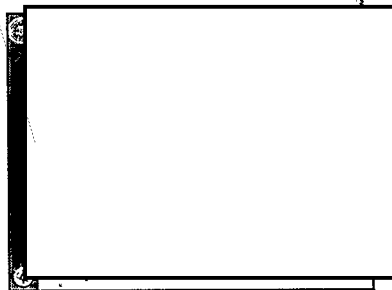
b1
b7E

(S)

(S)



(S)



b1
b7E

~~SECRET~~

~~SECRET~~

(S)

Evaluating and [redacted]

- Responsibility of the Case Agent
- Know the CI Program Strategy

[redacted]

FBI Training Center [redacted] 19

(S)

Exercise #2

[redacted]

FBI Training Center [redacted] 20

(S)

Elements of [redacted]

[redacted]

- Evaluation of interview results & investigative findings

FBI Training Center [redacted] 21

b1
b7E

(S)

Elements of [redacted]

- Records checks

[redacted]

- Re-checks

FBI Training Center [redacted] 22

(S)

Elements of [redacted]

- Direct
 - People
 - Places
 - Things
 - Information
- Indirect
 - People
 - Places

FBI Training Center [redacted] 23

(S)

Elements of [redacted]

- Preparation

[redacted]

- Post-interview Evaluation

FBI Training Center [redacted] 24

b1
b7E

(S)

Elements of [redacted]

- Determine need/requirement to interview

[redacted]

Considerations for interview

- Subject isn't cooperative or is hostile
- Diplomatic protest
- Negative publicity

FBI Training Center [redacted] 25

(S)

Elements of [redacted]

- The Approach
- Initial Contact
 - Going it alone
 - Direct or pretext?
- Location
- Cultural concerns and issues

FBI Training Center [redacted] 26

(S)

Elements of [redacted]

Questions

- Theirs
- Yours
- Problems during interview
- Denials/inconsistencies
- Challenge

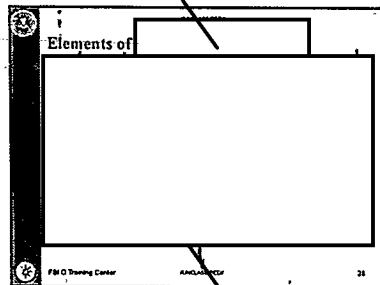
FBI Training Center [redacted] 27

b1
b7E

~~SECRET~~

~~SECRET~~

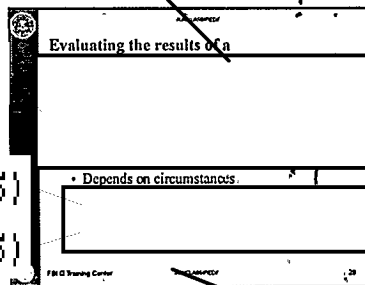
(S)



(S)

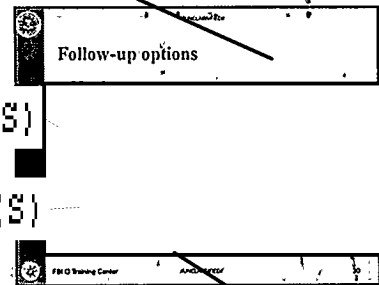
(S)

(S)



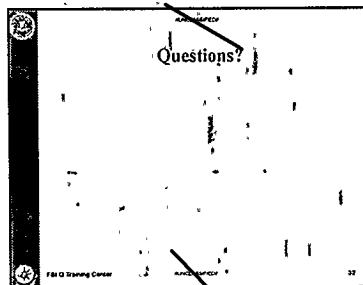
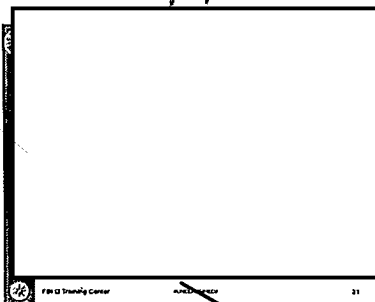
(S)

(S)



b1
b7E

(S)



b1
b7E

~~SECRET~~

~~SECRET~~

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

**Counterintelligence Cases:
CI Interviewing**

*Planning and Conducting
Counterintelligence Interviews*

FBI Training Center

What is a CI interview?

- **Definition:**
A planned and structured conversation with an individual designed to gather information so evidence can be collected or intelligence elicited that can be used to structure or further an investigation.

FBI Training Center

How do they differ from Criminal interviews?

- No crime is known to have occurred
- Interviewees cannot be compelled to talk to the FBI
- Category of person interviewed is generally different from persons involved in routine matters

FBI Training Center

What is a successful CI interview?

- It accomplishes CI interview objectives
- The interviewee is willing to be recontacted

FBI Training Center

**Why are CI interviews conducted?
CI Interview Objectives**

(S)

FBI Training Center

Why are CI interviews conducted?

- Acquire knowledge about patterns of activities (tradecraft) undertaken by foreign adversaries to locate and acquire restricted access information

FBI Training Center

b1
b7E

Why are CI interviews conducted?

- Potential for far-reaching consequences -

FBI Training Center

CI Interview Planning

- Planning is a detailed method formulated beforehand for doing something -

FBI Training Center

Elements of a CI Interview Plan

- Preparation
- Post-Interview Evaluation

FBI Training Center

b1
b7E

~~SECRET~~

~~SECRET~~

Preparation

- Doing those things that will make you ready to conduct a the CI interview
- Conduct Research on the
 - Predication of the interview
 - Investigative area of interest
 - Subject

FBI Q Training Center

The Subject

- Language
- Ethnic and cultural considerations
 - Names
 - Gender
 - Habits
 - Physical issues
 - Dietary customs and rules
 - Religious matters
 - Occupation
- Is approval needed to interview?

FBI Q Training Center

Preparation – Sources for background information on Subject

- Basic law enforcement checks
 - DMV
 - FBI indices including ELSUR
 - Criminal
 - Credit
- Public Sources
 - Lexis-Nexis
 - Internet
 - Professional publications/associations

FBI Q Training Center

b7E

Preparation – Sources for background information on Subject

- US Government
- US Intelligence Community

FBI Q Training Center

Execution – How are you going to conduct the interview?

FBI Q Training Center

Execution

FBI Q Training Center

b7E

Preparation – Initiation of CI interviews

- Who will know
 - Daily associates
 - Subordinates
 - Supervisors
 - Family
 - Neighbors
- What this is about and Why
 - Direct
 - Pretext

FBI Q Training Center

Preparation – Initiation of CI interviews

- Location – must be determined in the initial contact stage
 - Work
 - Residence
 - FBI office
 - Other

FBI Q Training Center

The Interview Questions

- Preparation requires that you think through both the
 - Questions subject is likely to ask and
 - Questions you want to ask

FBI Q Training Center

~~SECRET~~

~~SECRET~~

The Interview Questions

- Questions – Theirs
 - Who are you?
 - What are you doing here?
 - Why does the FBI want to talk to me?
 - Have I done something wrong?
 - How do you know what you know?
 - Who knows you are talking to me?
 - What do you know that I think I should know?
 - What should I do next?

FBI Training Center

ANGLAMPREV

19

The Interview Questions

- Questions – yours
 - Corroborate what you know about
 - Interviewee
 - Situation that generated the interview
 - Subjects know to interview
 - Corroboration is a test of interviewee's veracity
 - BUT do not discount faulty memory or information you have may be incorrect
 - Fill in the gaps
 - Identify and address conflicting information

FBI Training Center

ANGLAMPREV

20

The Interview Questions

- Questions – Yours
 - Subject's personal background
 - Name & identifying information
 - Education
 - Military
 - Volunteer work
 - Travel
 - Family information (look for derivative access)
 - Immediate
 - Parents and other relatives & locations

FBI Training Center

ANGLAMPREV

21

The Interview Questions

- Questions – Yours
 - Occupation/Employment
 - Full time/part time
 - Time on the job
 - Locations
 - Nature of work
 - Travel
 - Contacts with CI targets of interest
 - Professional contacts

FBI Training Center

ANGLAMPREV

22

Post-Interview Evaluation

- Have objectives been met?
 - Potential threat to national security?
- Was assessment info collected?
- Acquired [redacted]
- Asset potential?

FBI Training Center

ANGLAMPREV

24

b1
b7E

Communication

- Two types of personal communication
 - Verbal
 - Non-verbal – the majority of communication is expressed non-verbally
- You can identify verbal and non-verbal cues indicative of interviewee's mindset
- ...and you display cues too!

FBI Training Center

ANGLAMPREV

25

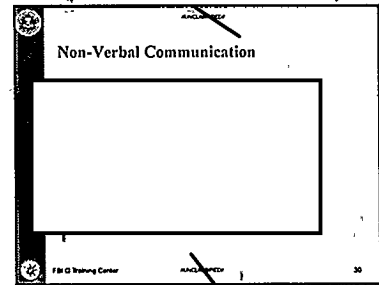
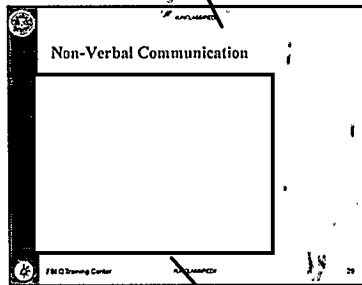
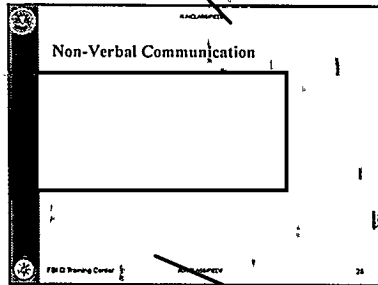
Non-Verbal Communication

Non-Verbal Communication

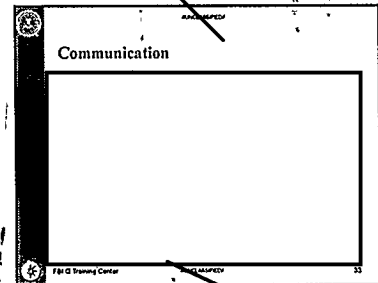
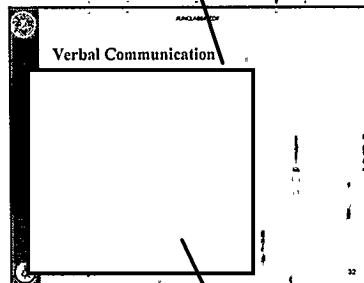
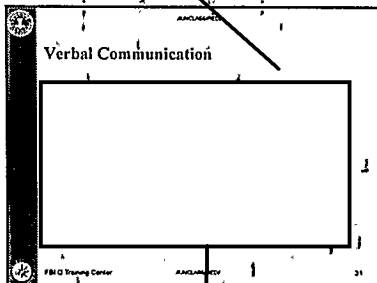
b7E

~~SECRET~~

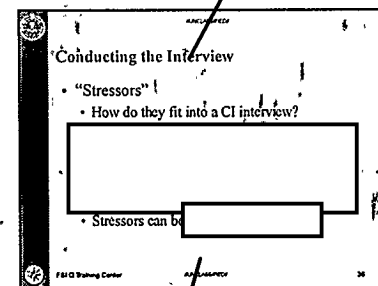
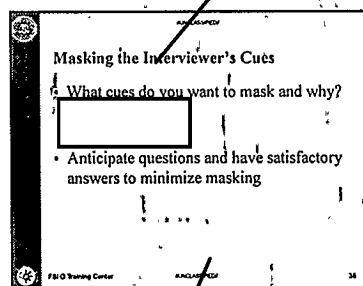
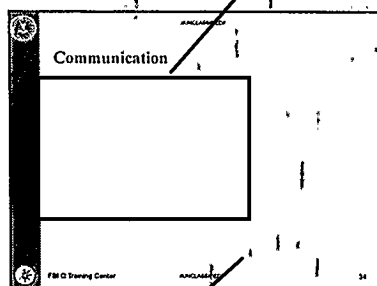
~~SECRET~~



b7E



b7E

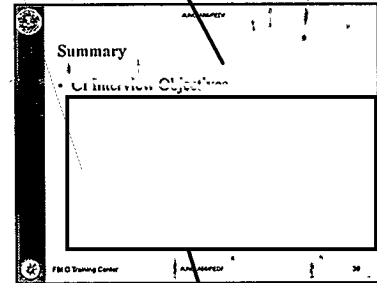
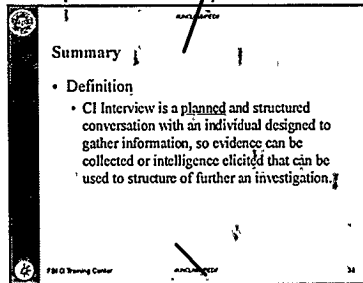
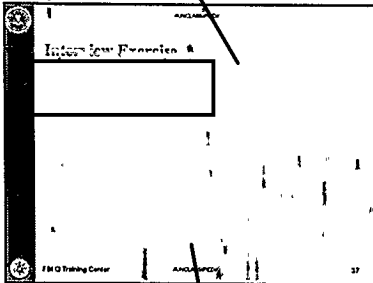


b7E

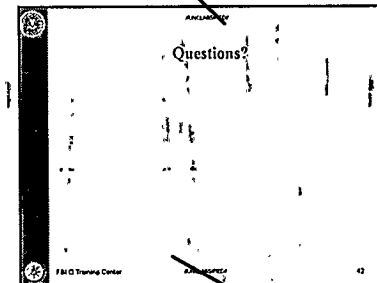
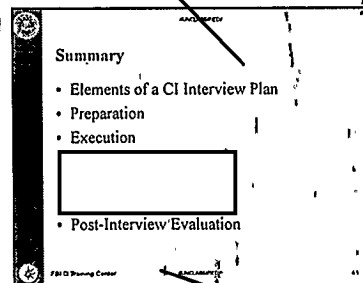
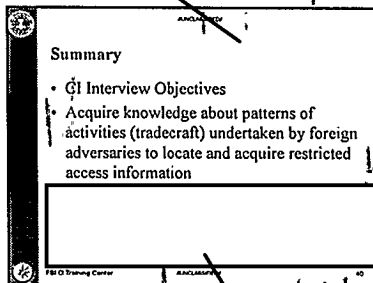
~~SECRET~~

~~SECRET~~

(S)



b1
b7E



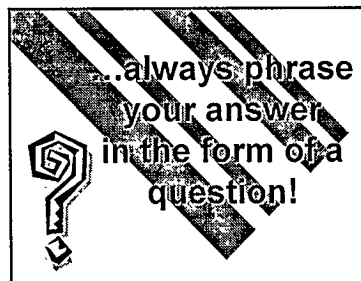
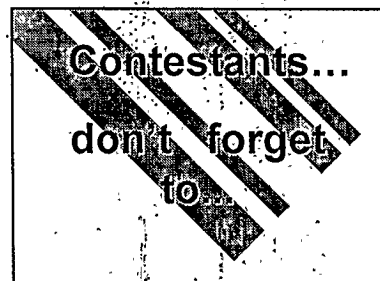
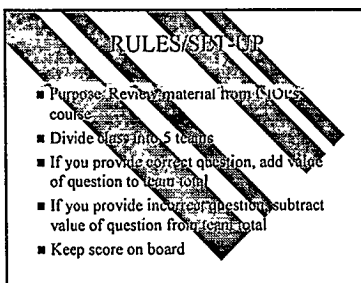
b7E

~~SECRET~~

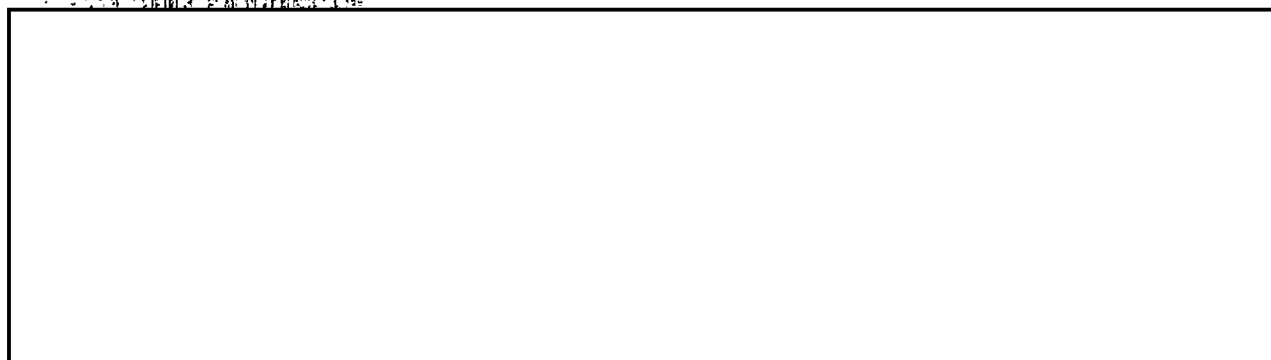
DATE: 02-14-2012
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 02-14-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE



100	100	100	100	100	100	100	100
200	200	200	200	200	200	200	200
300	300	300	300	300	300	300	300
400	400	400	400	400	400	400	400
500	500	500	500	500	500	500	500



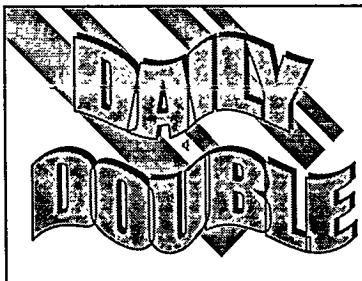
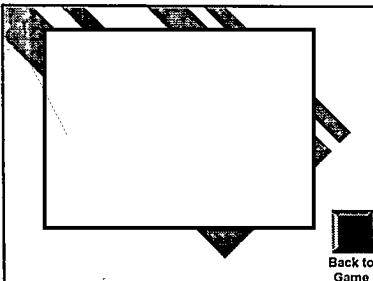
b7E

~~SECRET~~

ACLURM043698

~~SECRET~~

(S)



b1
b7E



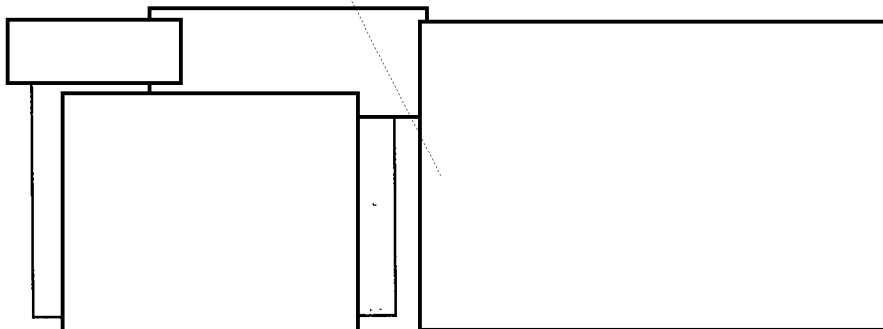
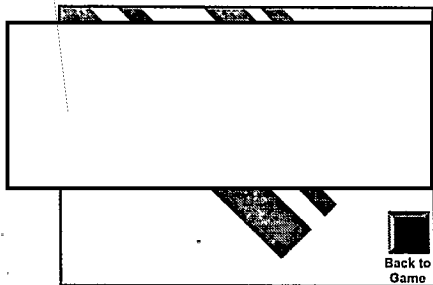
b7E

~~SECRET~~

~~SECRET~~

(S)

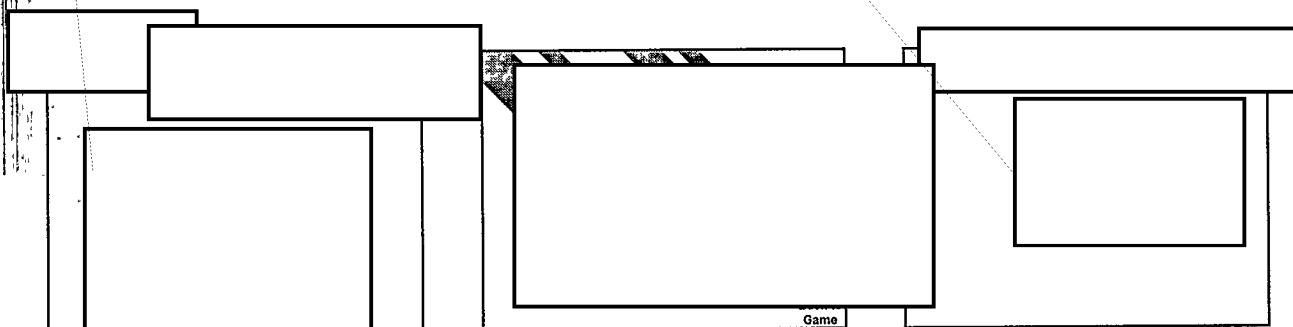
(S)



b1
b7E

(S)

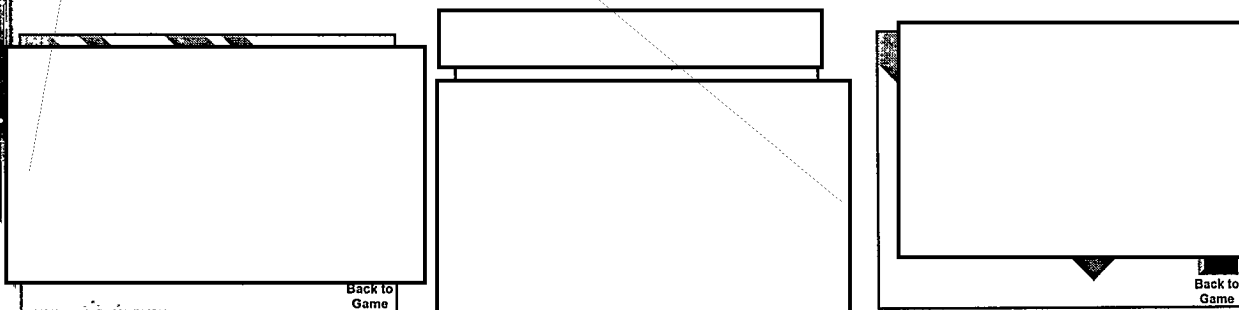
(S)



b1
b7E

(S)

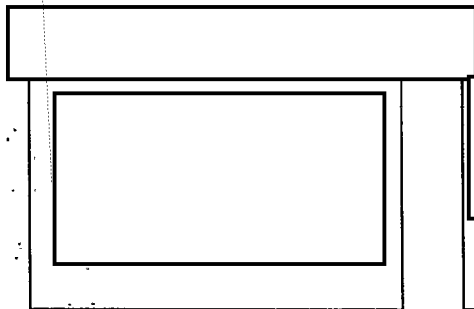
(S)



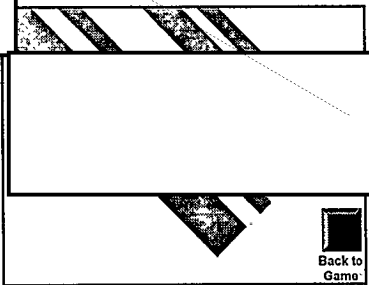
~~SECRET~~

~~SECRET~~

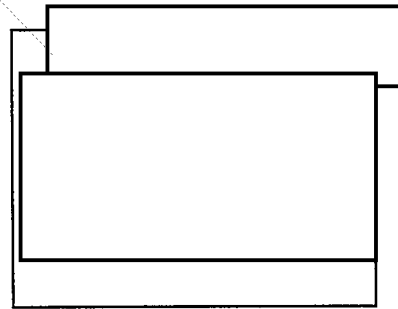
(S)



(S)

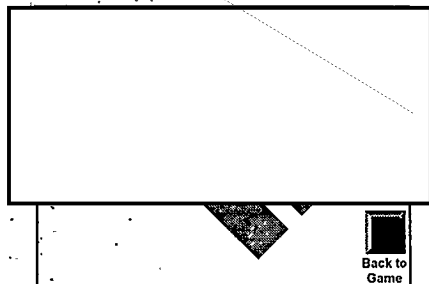


(S)

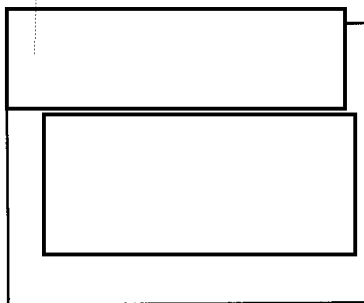


b1
b7E

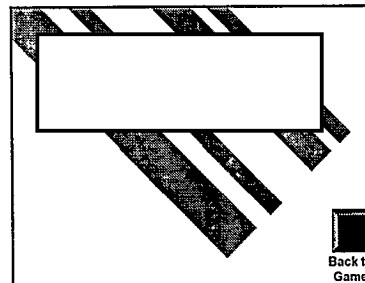
(S)



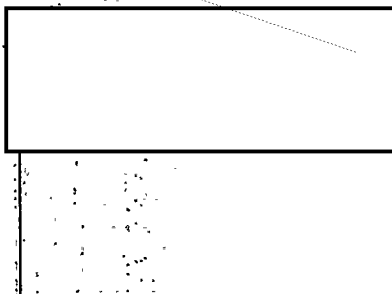
(S)



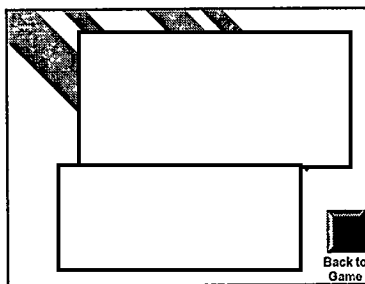
b1
b7E



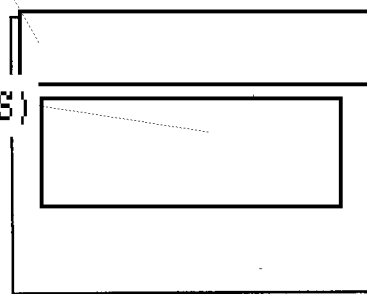
(S)



(S)



(S)



b1
b7E

~~SECRET~~

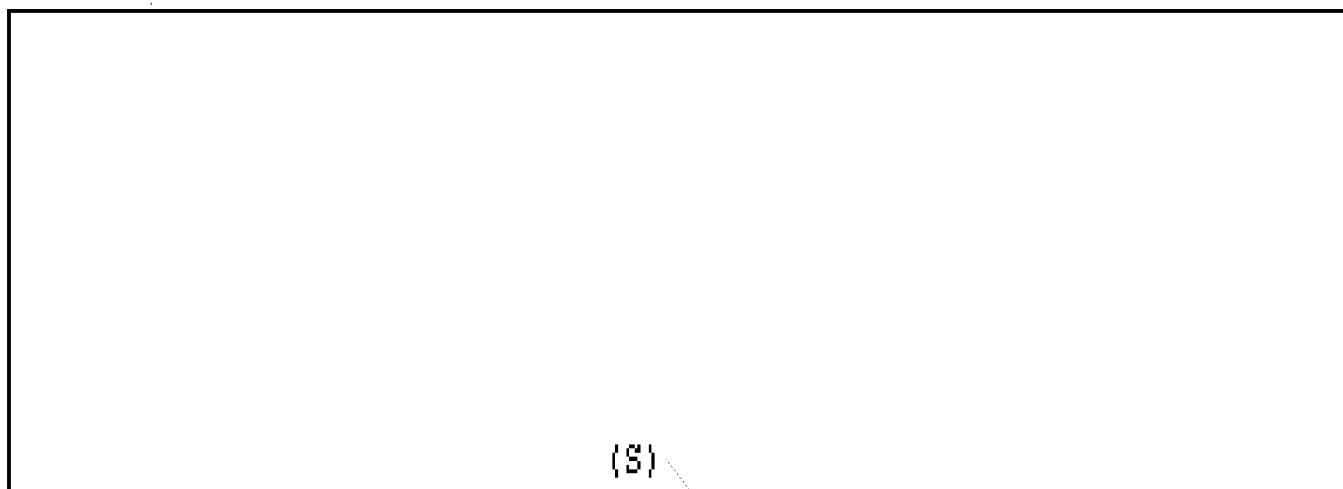
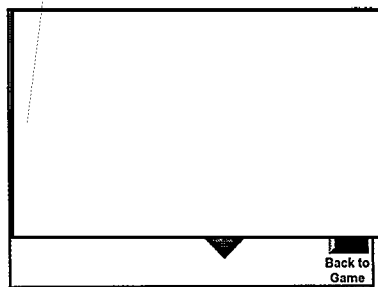
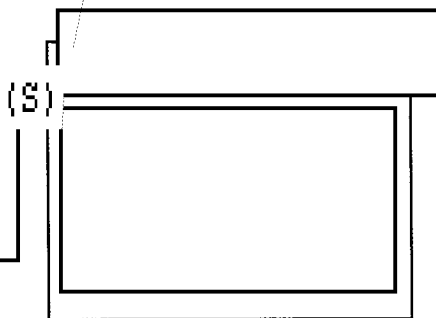
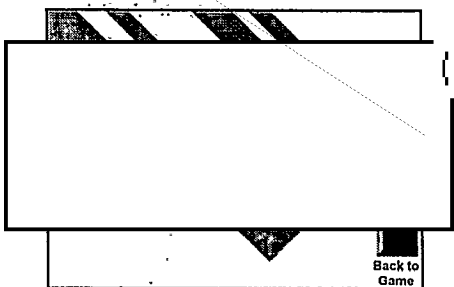
~~SECRET~~

(S)

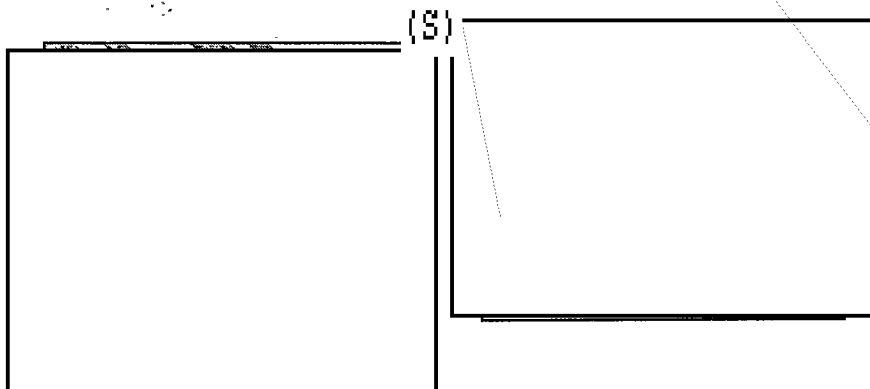
(S)

(S)

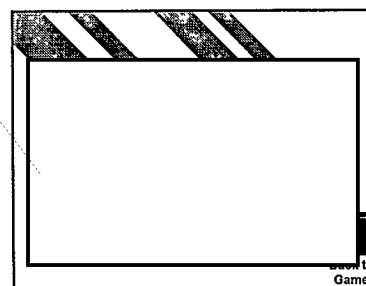
b1
b7E



b7E



(S)

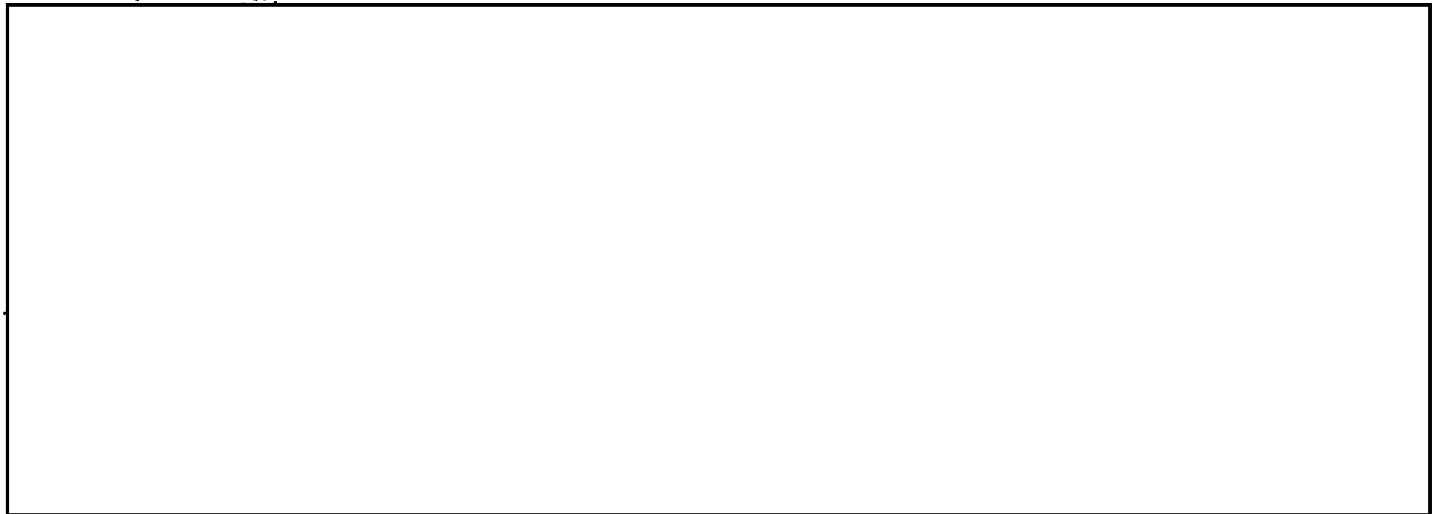


b1
b7E

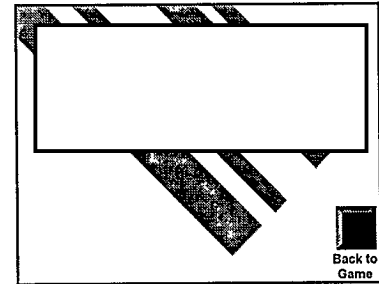
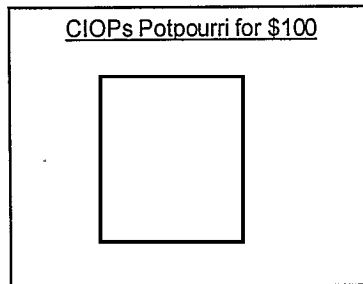
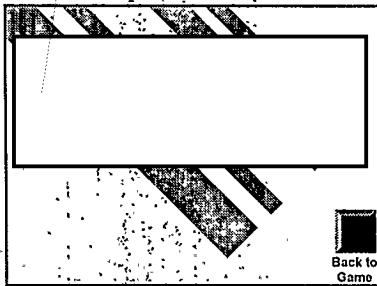
~~SECRET~~

~~SECRET~~

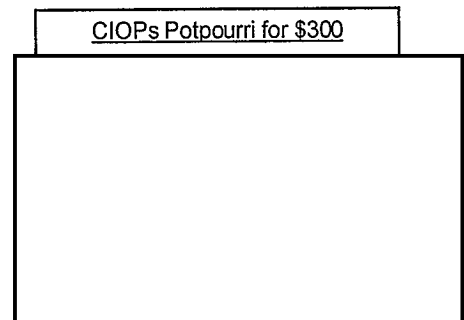
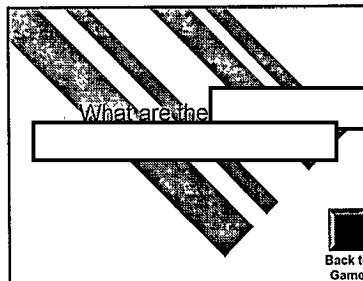
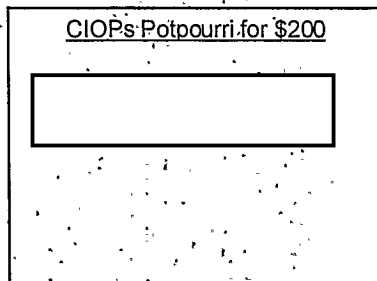
b7E



(S)

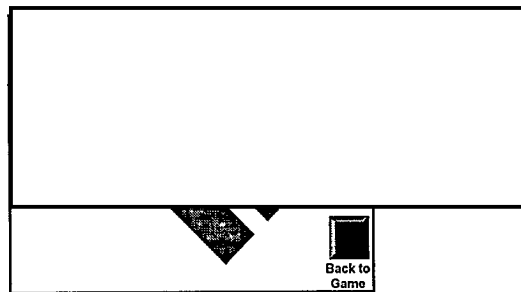
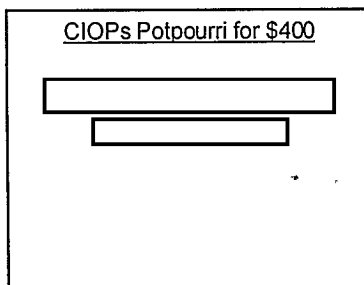
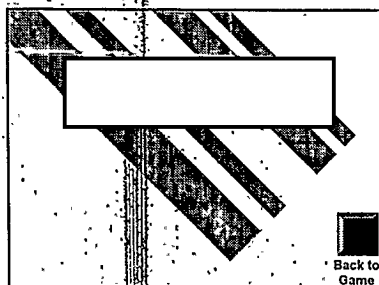


b1
b7E



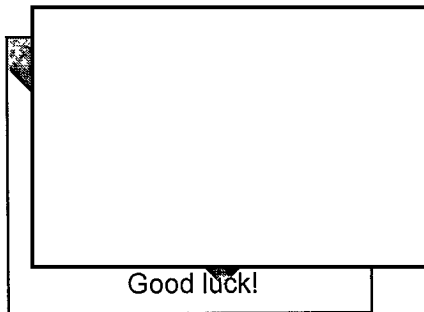
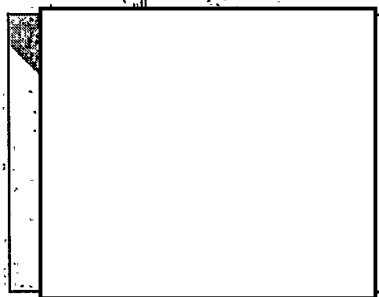
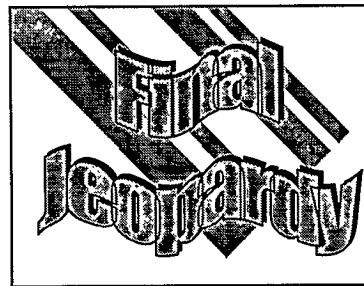
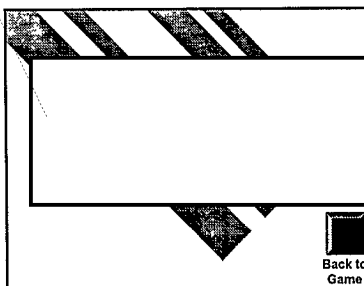
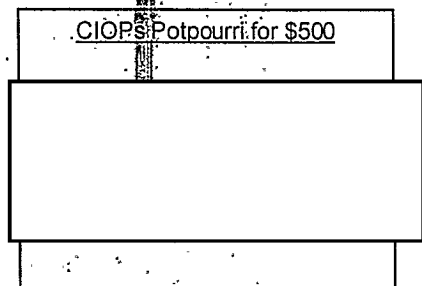
~~SECRET~~

~~SECRET~~



b1
b7E

(S)



b7E

~~SECRET~~

Serial Description ~ Unrecorded Serial

No. 100-42005
Page 100