



~~SECRET~~

National Security Investigations: The FBI's Investigative Priority

DATE: 03-07-2012
CLASSIFIED BY 65179 DMH/CLS
REASON: 1.4 (c)
DECLASSIFY ON: 03-07-2037

~~SECRET//NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET~~



Top Ten 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, county, municipal, and international partners.
10. Upgrade technology to successfully perform the FBI's mission

~~SECRET//NOFORN~~



~~SECRET~~

Objectives

- Describe the types of NSIs conducted by FBI
- Describe the components of the National Security Branch
- Describe three levels of investigation

~~SECRET//NOFORN~~

~~SECRET~~



FBI Authorities

FBI has primary jurisdiction over operations in the US

- Executive Order 12333: FBI is the primary for CI in the US (includes counterterrorism)
- Presidential Decision Directive 39: FBI is lead in response to DT/WMD

~~SECRET//NOFORN~~

~~SECRET~~



National Security Branch

- Counterterrorism Division (CTD)
- Counterintelligence Division (CD)
- Directorate of Intelligence (DI)
- Weapons of Mass Destruction Division (WMDD)



b7E

~~SECRET//NOFORN~~



Types of NS Investigations

- Foreign Counterintelligence

- Foreign intelligence collection

- Espionage Criminal Investigations

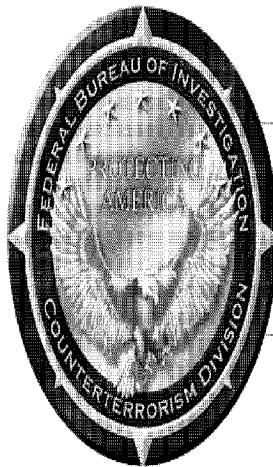
- Terrorism

- Domestic Terrorism

b7E

- International Terrorism

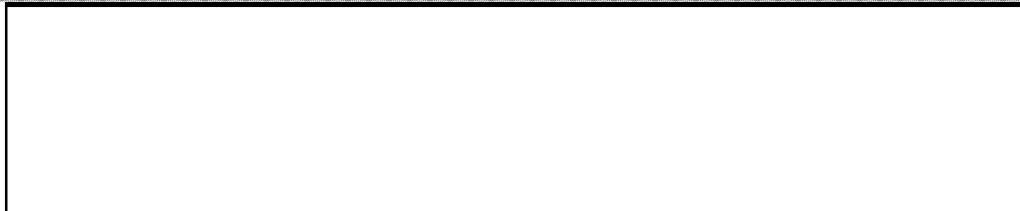
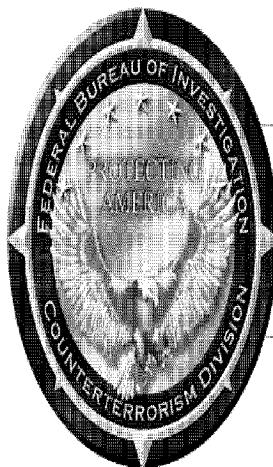
- Foreign Intelligence Collection



Counter vs. Foreign

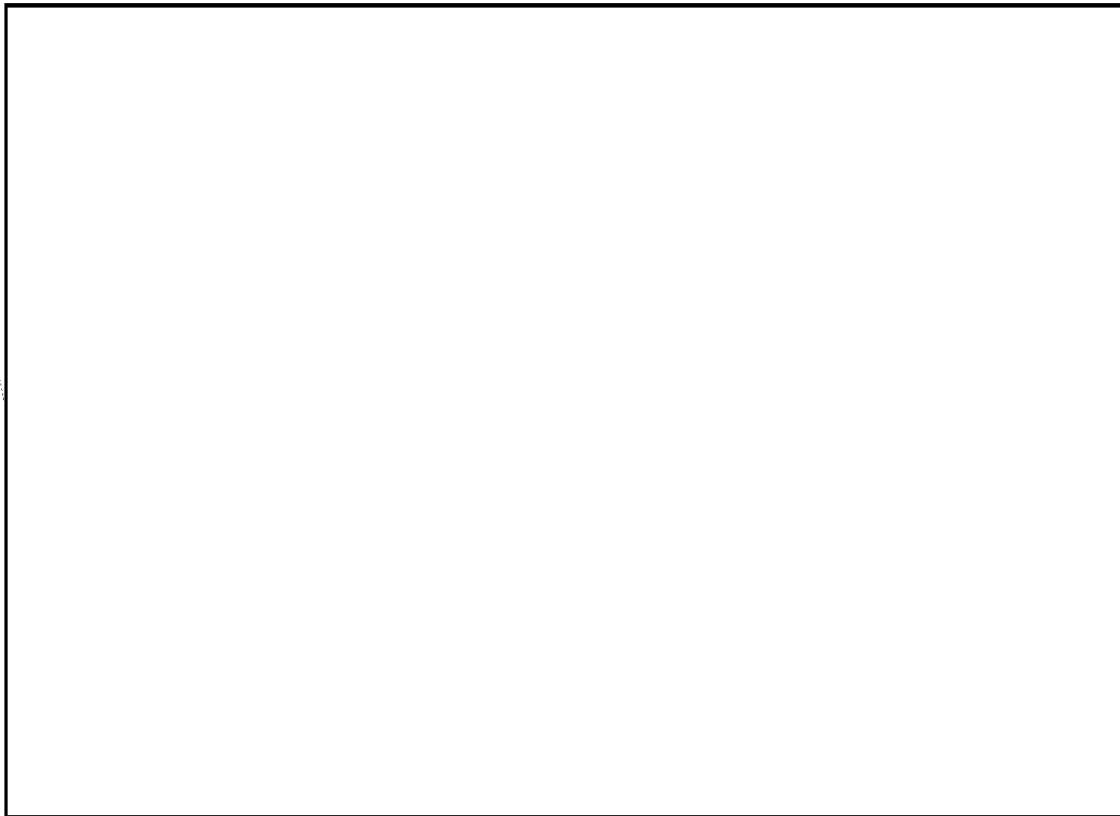
- **Counterintelligence** - Information gathered and activities conducted to protect against espionage, sabotage, and other intelligence activities conducted on behalf of foreign powers or by international terrorists
- **Foreign Intelligence** - Information related to the capabilities, intentions, and activities of foreign powers, organizations or persons, that does not include counterintelligence except for information on international terrorism matters.

~~SECRET~~



b7E

(S)



b1
b7D
b7E

~~SECRET//NOFORN~~

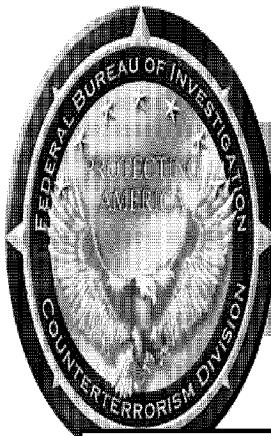


Counterintelligence Division Priorities

- Prevent or neutralize the foreign acquisition of weapons of mass destruction (WMD) technology or equipment;
- Prevent the penetration of the U.S. [redacted] Community;
- Prevent the penetration of U.S. Government agencies or contractors; and
- Prevent the compromise of U.S. Critical [redacted]
[redacted]

b7E

~~SECRET~~



Counterintelligence Sections

Section

Global Section

Section

Counterespionage Section

Administrative Section

b7E

Section

Section

Section

~~SECRET//NOFORN~~



~~SECRET~~

Identify, Penetrate, Neutralize

- Personnel
- Method of Operation
- Targets

~~SECRET//NOFORN~~

~~SECRET~~



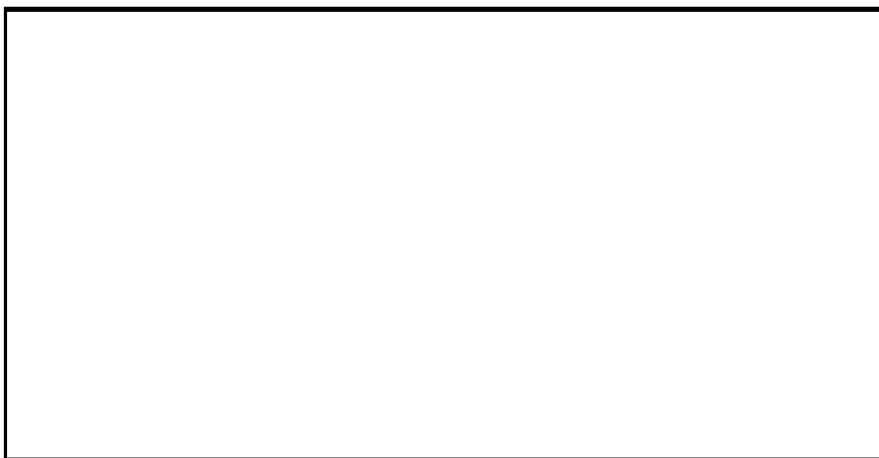
Identify, Penetrate, Neutralize

- Technical Penetration



- Bugs

- Human



b7E

~~SECRET//NOFORN~~

~~SECRET~~

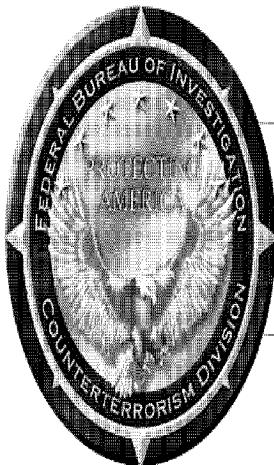


Identify, Penetrate, Neutralize

- Persona non Grata (PNG)
- Criminal Prosecution
 - Espionage Statute – Title 18, USC S794
 - Economic Espionage Act
 - Terrorism Statutes
 - Any possible federal statute, including Title 18, USC S 1001

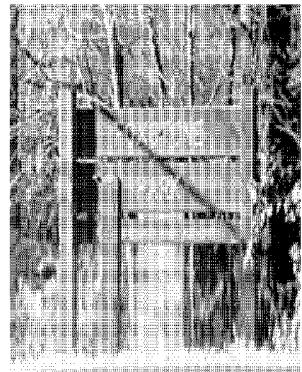
~~SECRET//NOFORN~~

~~SECRET~~



CI Major Case: Robert Hanssen

- Volunteered to USSR
- Long term investigation
- In 2000, a suspicious package identified
- 02/18/2001 Identified making dead drop and arrested
- 07/06/2001 Pled guilty to 15 espionage charges.



~~SECRET//NOFORN~~

~~SECRET~~



FBI

ROBERT P. HANSSEN (FBI)



A 56 year old veteran FBI employee who received more than \$1.4 million in cash and jewels while spying for 17 years for the KGB/SVR. He pled guilty to 15 counts of espionage-related charges. Sentence: life



~~SECRET~~



Counterterrorism Division

- Lead law enforcement and domestic intelligence efforts to defeat terrorism.
- Eliminate terrorists' ability to operate so people live without fear of terrorism

~~SECRET//NOFORN~~



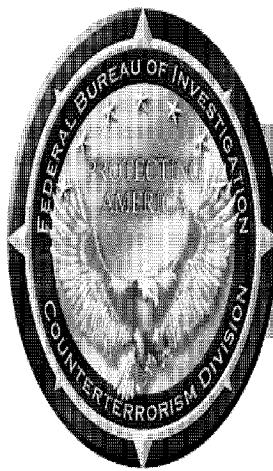
CTD Objectives

To detect, disrupt, and dismantle terrorist sleeper cells in the United States before they act;

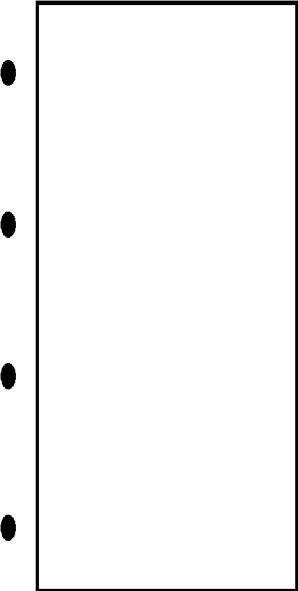
- To identify and prevent acts of terrorism by individuals with a terrorist agenda acting alone;
- To detect, disrupt, and dismantle terrorist support networks, including financial support networks;
- To enhance our capability to quickly ascertain the reliability, implications and details of terrorist threats and to improve our capacity to disseminate threat-related information to local, state, and federal agencies, and to the private sector as needed; and
- To enhance our overall contribution to the USIC and to senior policy makers in government by providing timely and accurate in-depth analysis of the terrorist threat and other information of value on an on-going basis.

~~SECRET//NOFORN~~

~~SECRET~~



State Sponsors of Terrorism

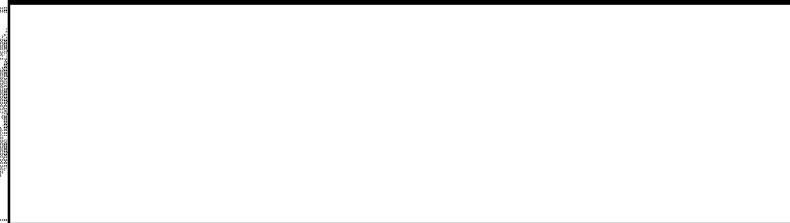


b7D

~~SECRET NOFORN~~



~~SECRET~~



b7E

- (U) • (S) Intelligence Community (IC) recognizes [redacted] terrorist groups operating worldwide

- (U) • (S) [redacted]
- [redacted]

b7E

~~SECRET//NOFORN~~

~~SECRET~~



Ranking Criteria

b7E

- (T) • (S) [redacted] ranking system based on the following factors:

[redacted]

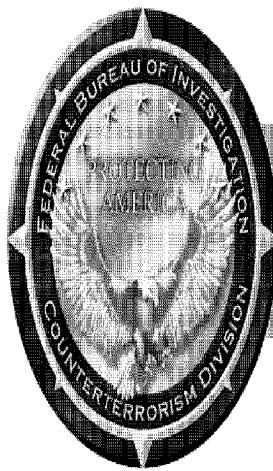
b7E

- Updated quarterly
- Two levels [redacted]

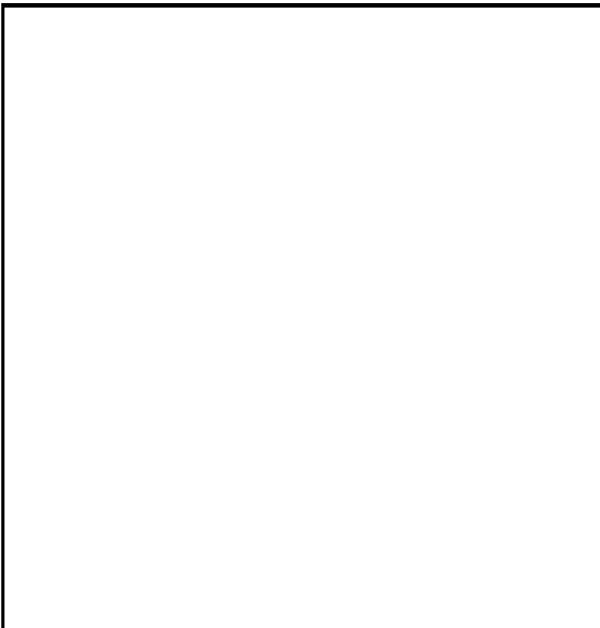
[redacted]

~~SECRET//NOFORN~~

~~SECRET~~



CTD Top Threats

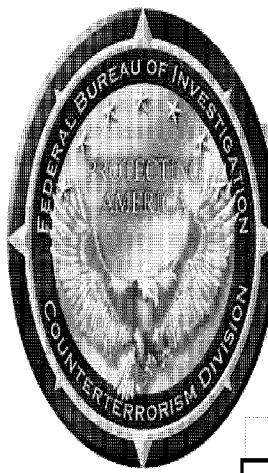


b7E

- Domestic Terrorism

~~SECRET//NOFORN~~

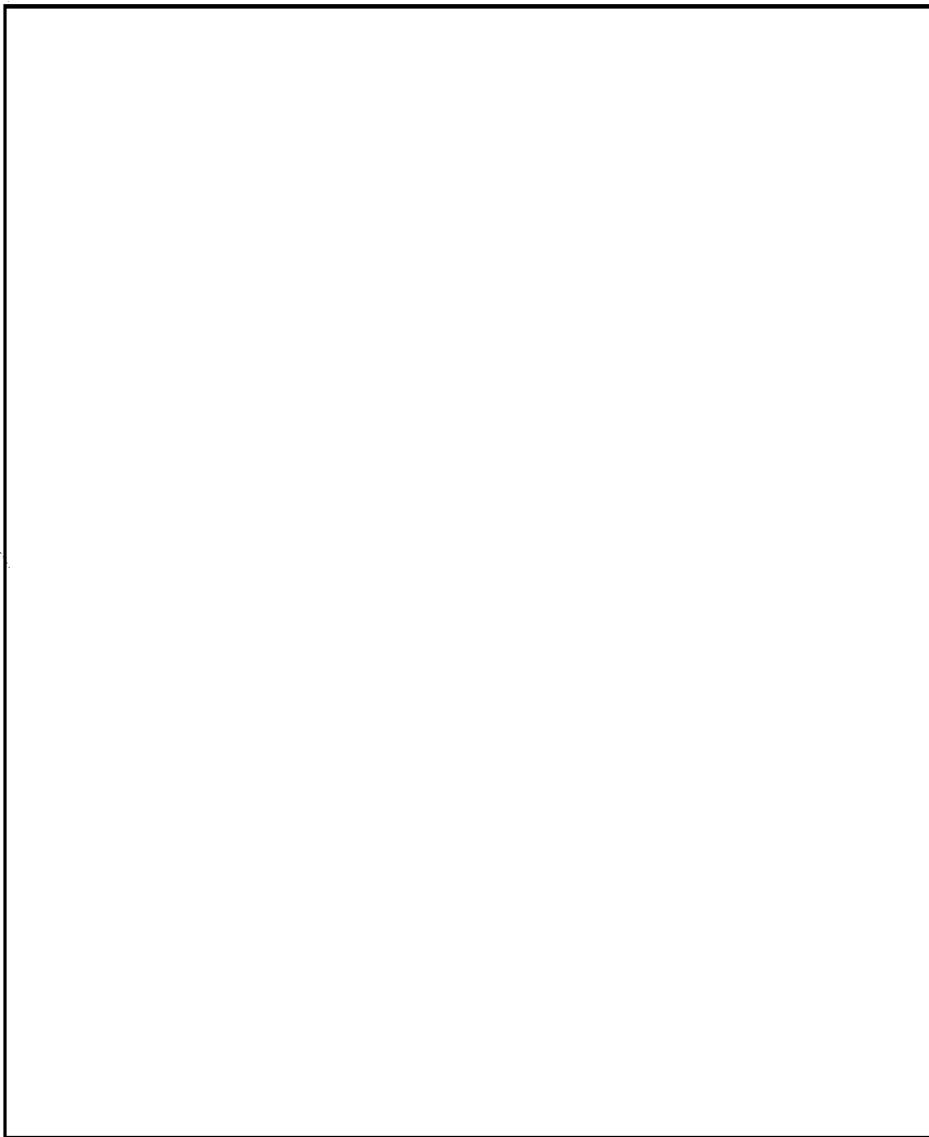
~~SECRET~~



Threat Prioritization

CTD Threat Prioritization Matrix

(S)



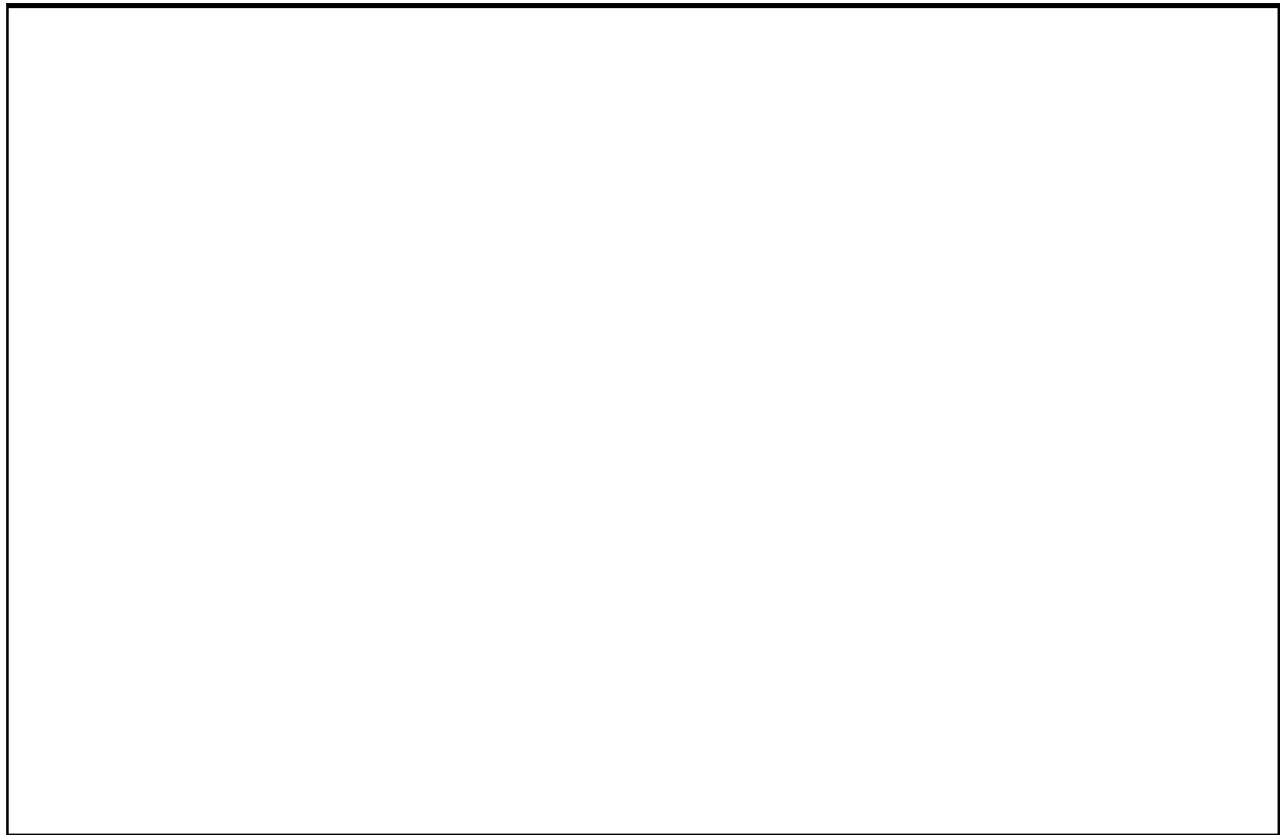
b1
b7E

~~SECRET NOFORN~~



~~SECRET~~

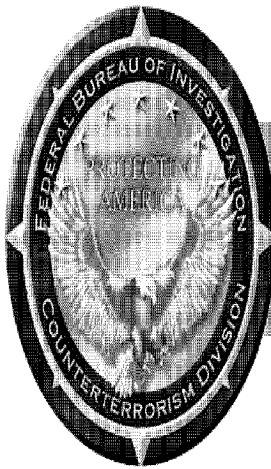
Countering Terrorist Groups



b7E

- Other support entities

~~SECRET//NOFORN~~



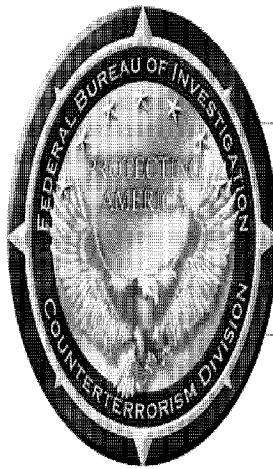
~~SECRET~~

Substantive Resource

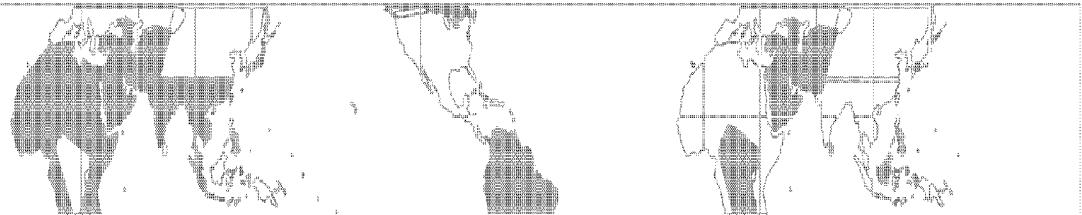
Subject Matter Expert (SME)

b7E

~~SECRET//NOFORN~~



~~SECRET~~



Case Predication and Levels of Investigation

~~SECRET//NOFORN~~



~~SECRET~~

Levels of Investigation

- Assessments
- Preliminary Investigations
- Full Investigations

~~SECRET//NOFORN~~



~~SECRET~~

A world map graphic showing the outlines of continents against a dotted background. The word "Assessments" is overlaid in large, bold, black font across the map.

Assessments

- Need to have an authorized purpose
- Cannot be based solely on First Amendment Rights

~~SECRET//NOFORN~~

~~SECRET~~



Six Assessment Types

- Type 1: Cover Investigative

- Type 2: Cover investigative

- Type 3: Identify

b7E

- Type 4: Conduct

- Type 5:

- Type 6:

~~SECRET//NOFORN~~

~~SECRET~~



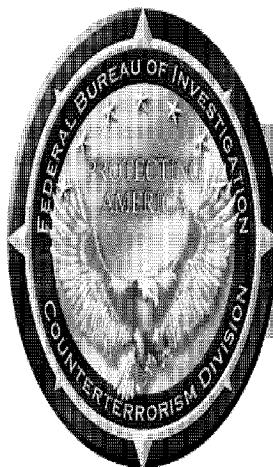
Assessments

- Scenarios to use



~~SECRET//NOFORN~~

~~SECRET~~



Preliminary Investigations

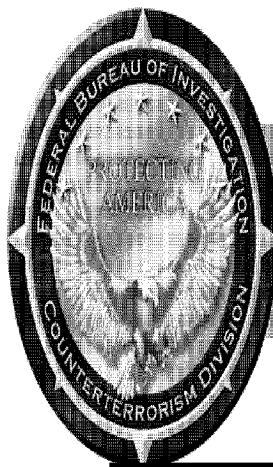
- Predication: information or allegation indicating a federal crime or threat to



b7E

~~SECRET//NOFORN~~

~~SECRET~~



NSI PI predictions

b7E

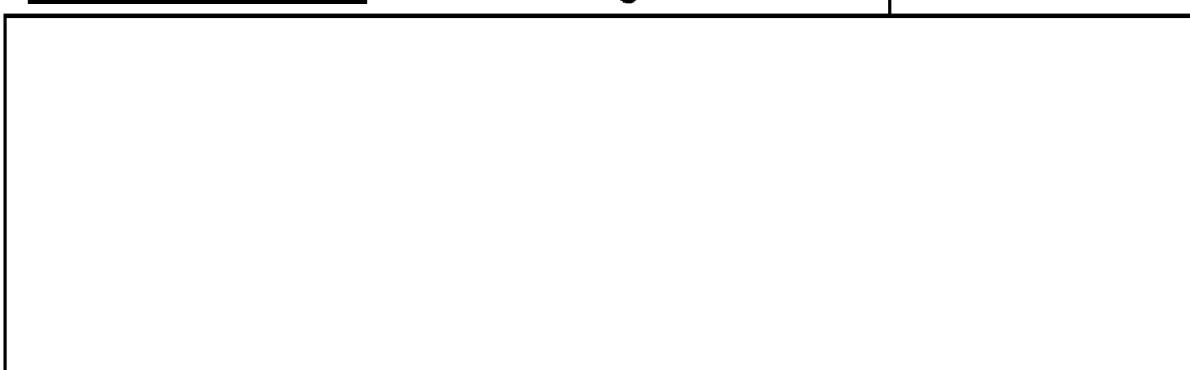
~~SECRET//NOFORN~~

~~SECRET~~



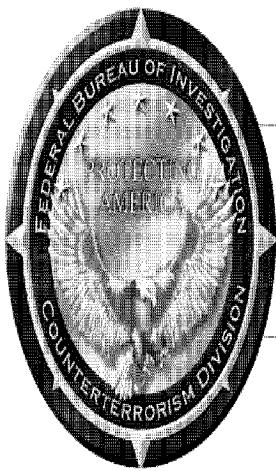
Full Investigations

- Predication: Articulable factual information indicating a threat

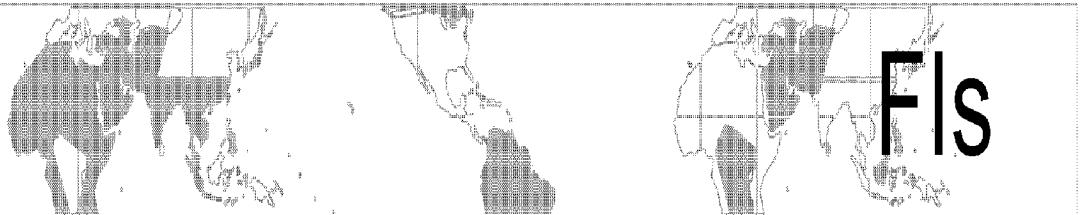


b7E

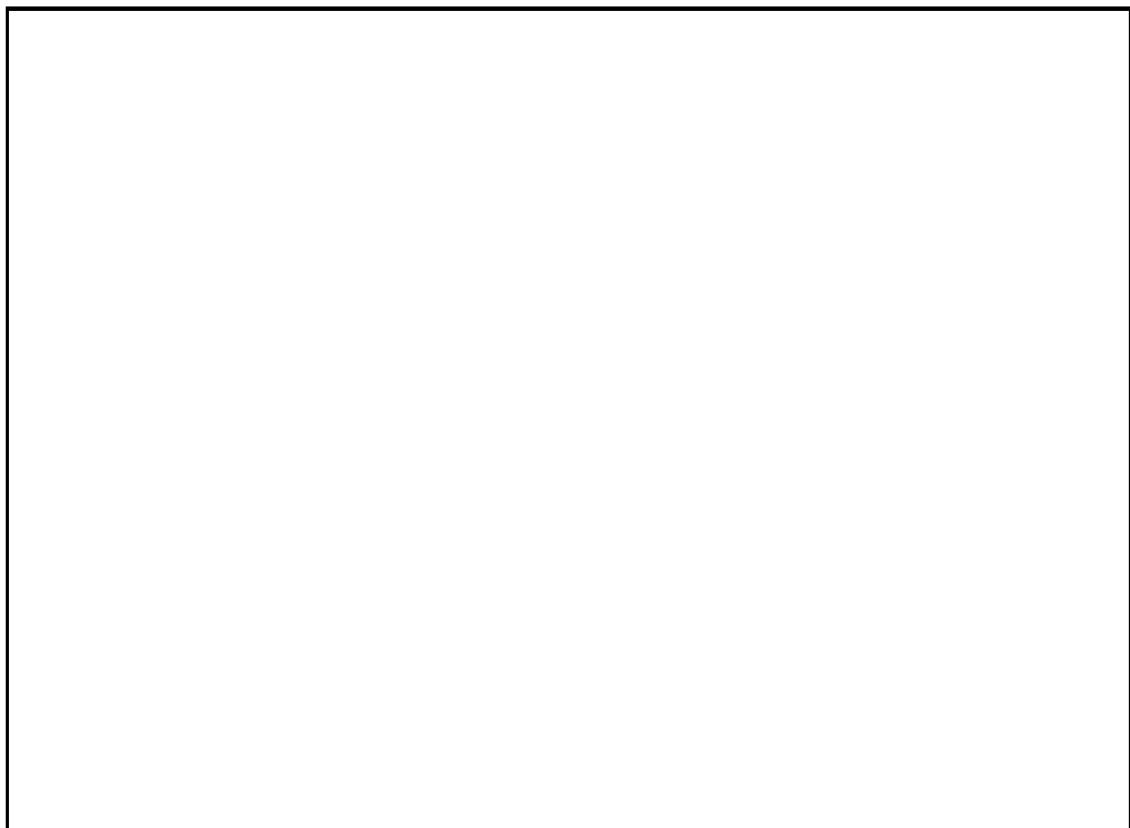
~~SECRET//NOFORN~~



~~SECRET~~



- Full Investigation = PI + Corroboration
 - CT Example:



~~SECRET//NOFORN~~



~~SECRET~~

Two Types of Unique FIs

- Foreign Intelligence Collection

- Must be approved by SAC
 - Conducted on the FIG

b7E

- Enterprise Operation Cases

- Investigate a Group for a coordinated criminal activity
 - Multiple subjects

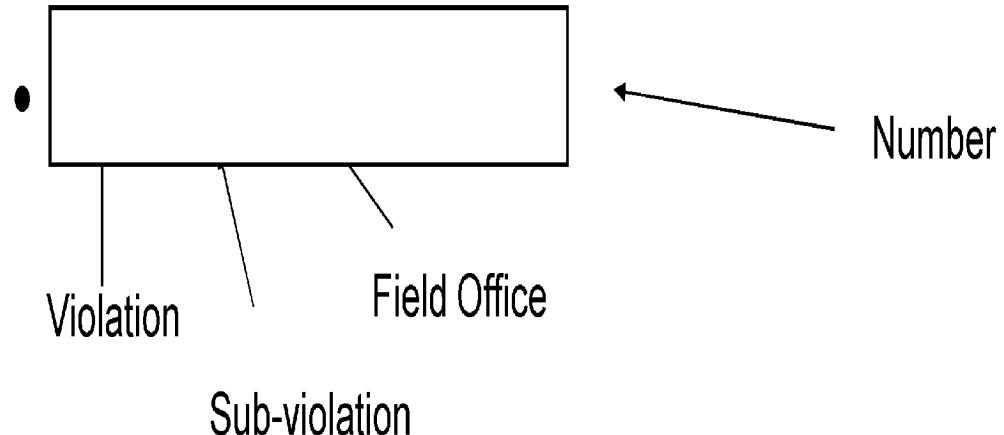
~~SECRET//NOFORN~~



~~SECRET~~

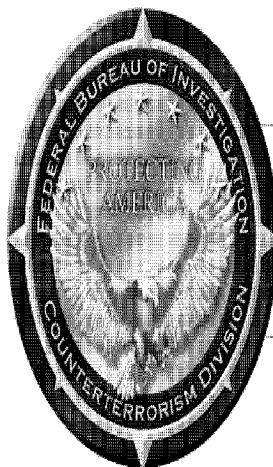
File Classification

- Determined by MIOG (Manual of Investigative Operations and Guidelines) and (NFIPM) National Foreign Intelligence Policy Manual



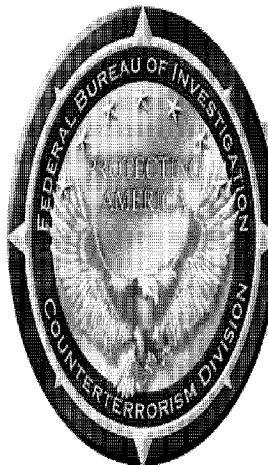
b7E

~~SECRET//NOFORN~~



Field Initiation

- Predication reviewed by SSA
- Opening Electronic Communication (EC) written
- Assigned Case Number by SST (Support Services Technician)
- Opening communication(s) uploaded and sent to HQ/file



Opening Communications

- EC required in order to open any case
- Letterhead Memorandums (LHMs) to DOJ/Office of Intelligence (OI) required for certain cases
- For CT [redacted]
[redacted] must be completed for entry in [redacted]
[redacted]

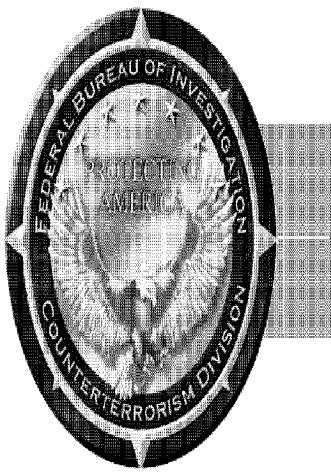
b7E

~~SECRET~~

Opening EC

- Required fields
 - Dates
 - Synopsis
 - Details
 - Identifiers
- Optional Fields
 - References
 - Enclosures
- Leads

~~SECRET//NOFORN~~

~~SECRET~~

(Re 01-01-2003)

~~SECRET//[Data from Declassify on Line]~~**FEDERAL BUREAU OF INVESTIGATION**

Precedence. ROUTINE

Date. 12/01/2006

To. Counterterrorism

Attn. Operational Section/Unit

	Rm. 4933

b7E

To:
Division

From. New York

Squad 505
Contact. SA [redacted] Agent, (xxx) xxx-xxxx

Approved By. [redacted]

Drafted By. Agent [redacted] jqa

Case ID #. (U) [redacted] (Pending)

b6
b7C
b7E

Approval Line

Title. (S) [redacted]

Case Title

Synopsis. (S) [redacted]

Declassification Date

(U) Derived from. FBI 806 #3, Jan 1997
Declassify On. [25 years from date of 806]

Synopsis: To open investigation

[Note. Portion mark each paragraph, including subparagraphs, based on content of the portion. The portion markings shown in this example are for illustration only.]

Enclosure(s). (U) There are two enclosures: (1) The Notice of Initiation for [Operational section/unit] (example: [redacted] (submitted via [redacted]); and (2) Electronic [redacted] for the [redacted] Unit (submitted via email only to [redacted])

Enclosures

b7E

[Expedited Requests: If a subject needs to [redacted]
[redacted] please call [redacted] to advise the [redacted] staff; email a completed [redacted] the supporting documentation to the person you spoke to, copy the [redacted] Unit mailbox at [redacted] and mark the message urgent, "Please Expedite!"]

b7E

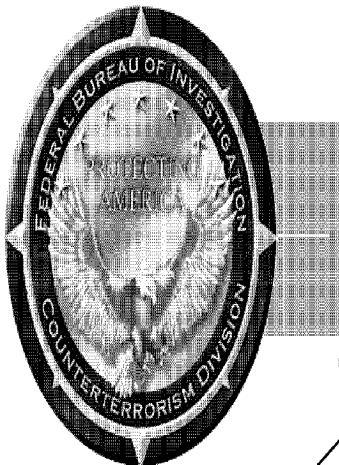
~~SECRET//[Data from Declassify on Line]~~

ACLURM050021

~~SECRET~~

43

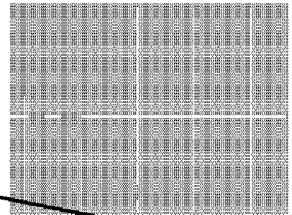
FBI050433

~~SECRET~~

b7E

To: Counterterrorism From: New York
Re: (U) [REDACTED] 12/01/2006

Preliminary (or Full) Investigation Initiated. 01/13/2005



Details. (S) New York is opening the captioned Preliminary (or Full) Investigation . . .

(Note: The opening EC should be rich in detail, whereas the narrative in the Notice of Initiation should be no more than a paragraph or two. [REDACTED] include the following in the Miscellaneous field: the case agent's name and 24/7 contact number, [REDACTED] and any other pertinent information.)

Date
Investigation
Initiated

b7E

Body of EC
Begins here

Predication for the Investigation

(S) This section should describe any investigative activity conducted during a Threat Assessment which led to the initiation of the case and clearly articulate the predication.

(U) Preliminary Investigations are authorized, generally speaking, when there is information or an allegation [REDACTED] indicating that a threat [REDACTED]

b7E

(U) Full Investigations are authorized, generally speaking, when there are specific and articulable facts giving reason to believe that a threat [REDACTED]

b7E

(U) The circumstances on which the initiation of a preliminary investigation or full investigation may be based are:

→

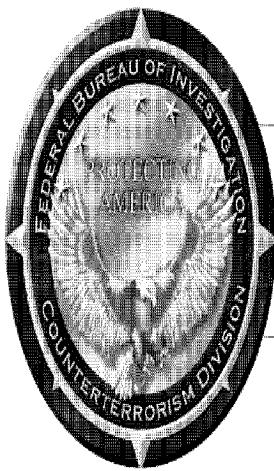
Options for
Predication

[REDACTED]

b7E

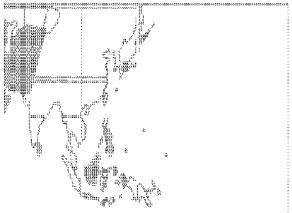
~~SECRET~~

ACLUJRM050922

~~SECRET~~

b7E

To: Counterterrorism From: New York
Re: (U) [REDACTED] 12/01/2006



b7E

Possible Nexus to a Foreign Power

(S) This section should specify the known or suspected foreign power.

(U) A "foreign power" is defined as:

1. (U) a foreign government or any component thereof, whether or not recognized by the United States;
2. (U) a faction of a foreign nation or nations, not substantially composed of United States person;
3. (U) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or government;
4. (U) a group engaged in international terrorism or activities in preparation therefor;
5. (U) a foreign-based political organization, not substantially composed of United States person; or
6. (U) an entity that is directed or controlled by a foreign government or governments.

Partinent Sensitive National Security Matters

(U) "Sensitive National Security Matter" is defined as:

A threat to the national security involving the activities of

should be brought to the attention of FBI Headquarters and other Department of Justice officials.

(U) If there are none known, then simply state: "There are no known sensitive national security matters."

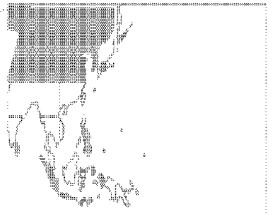
~~SECRET~~~~SECRET~~



~~SECRET~~

b7E

To: Counterterrorism From: New York
Re: (U) [redacted] 12/01/2006



Known Identifiers

(U) In addition to the data fields in the Descriptive Data portion of the BC macro, include all known identifiers about the subject in this section.

(U) It is critical that all information be indexed [redacted]

a)

[redacted] Osama bin Laden's full name, for example, is Osama bin Mohammad bin Abdallah bin Laden

b)

c)

d)

e)

f)

g)

h)

i)

j)

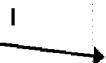
k)

l)

m)

n)

Descriptive Data.



Subject identifiers

(U) Main Subject

b7E

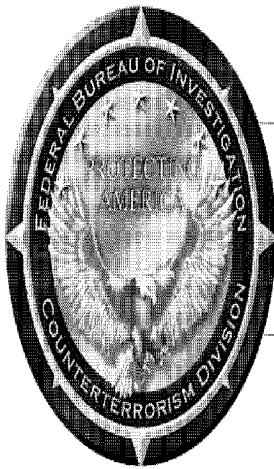
~~SECRET~~

~~SECRET~~

ACLURM050924

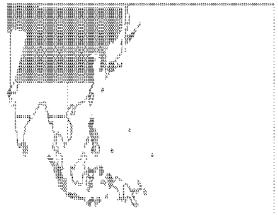
46

FBI050436

~~SECRET~~

b7E

To: Counterterrorism From: New York
Re: (U) [redacted] 12/01/2006



LEAD(s).

Set Lead 1. (Action)

COUNTERTERRORISMAT WASHINGTON, DC

(S) [operational section/unit] is requested to provide notice of the initiation of this investigation to the DDCI [redacted]
[redacted]

b7E

Set Lead 2. (Action)

COUNTERTERRORISMAT WASHINGTON, DC

(S) [operational section/unit] coordinate [redacted]
[redacted] as required based on information in Details, above.

b7E

Set Lead 3. (Action)

COUNTERTERRORISMAT WASHINGTON, DC

(U) [redacted]
[redacted] is requested to process [redacted] which is being submitted via email to the [redacted] mailbox [redacted] to add the subject of this case to the [redacted]
[redacted] appropriate supported systems.

b7E

Set Lead 4. (Info)

COUNTERTERRORISMAT WASHINGTON, DC

(U) CT Analysis Section: Read and clear.

~~SECRET~~

6

~~SECRET~~

~~SECRET~~



- Serial 1: Opening EC
- Serial 2: for certain NSI cases, LHM
- All other serials proceed from least to more invasive
- All investigation must be documented to file
- Each document given a serial number, written on lower left corner.
- Each document has at least one unique number: combination of file number and serial number

~~SECRET NOFORN~~



~~SECRET~~

Types of Serials

- ECs



b7E

- Physical Surveillance (FISUR) log
- National Security Letters (NSLs)
- Teletypes/Cables
- Letterhead Memorandums (LHMs)
- Mail cover (request and results)
- other government agencies results
- 1A envelopes (FD-340)

~~SECRET//NOFORN~~



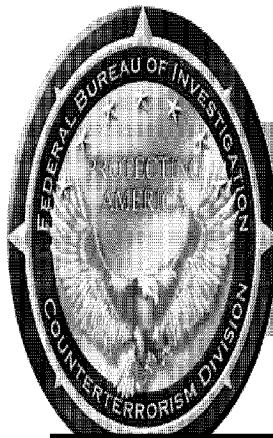
~~SECRET~~

Subfiles

- Used to group similar information together in the case file
- Documents in subfiles must be serialized
- Serialized beginning at Serial 1 for each subfile (serials are separate from main file)

~~SECRET//NOFORN~~

~~SECRET~~



Common Subfiles

- CRIM
- FISUR
- NSL
- GJ

b7E

~~SECRET//NOFORN~~

~~SECRET~~



Exercise

- Identify the proper type [redacted] and the level at which that investigation should be opened
- Don't forget that no investigation can be initiated only on activities protected by the First Amendment

b7E

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

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

Total Deleted Page(s) ~ 4

Page 14 ~ b1, b7E

Page 15 ~ b1, b7D, b7E

Page 23 ~ b1, b7E

Page 24 ~ b1, b7D, b7E