

~~SECRET~~

DATE: 10-05-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 10-05-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

COUNTERINTELLIGENCE



THREAT PROGRAM GUIDE

b7E

GUIDANCE FOR MANAGING AND SUPERVISING THE CI [REDACTED] THREAT PROGRAM

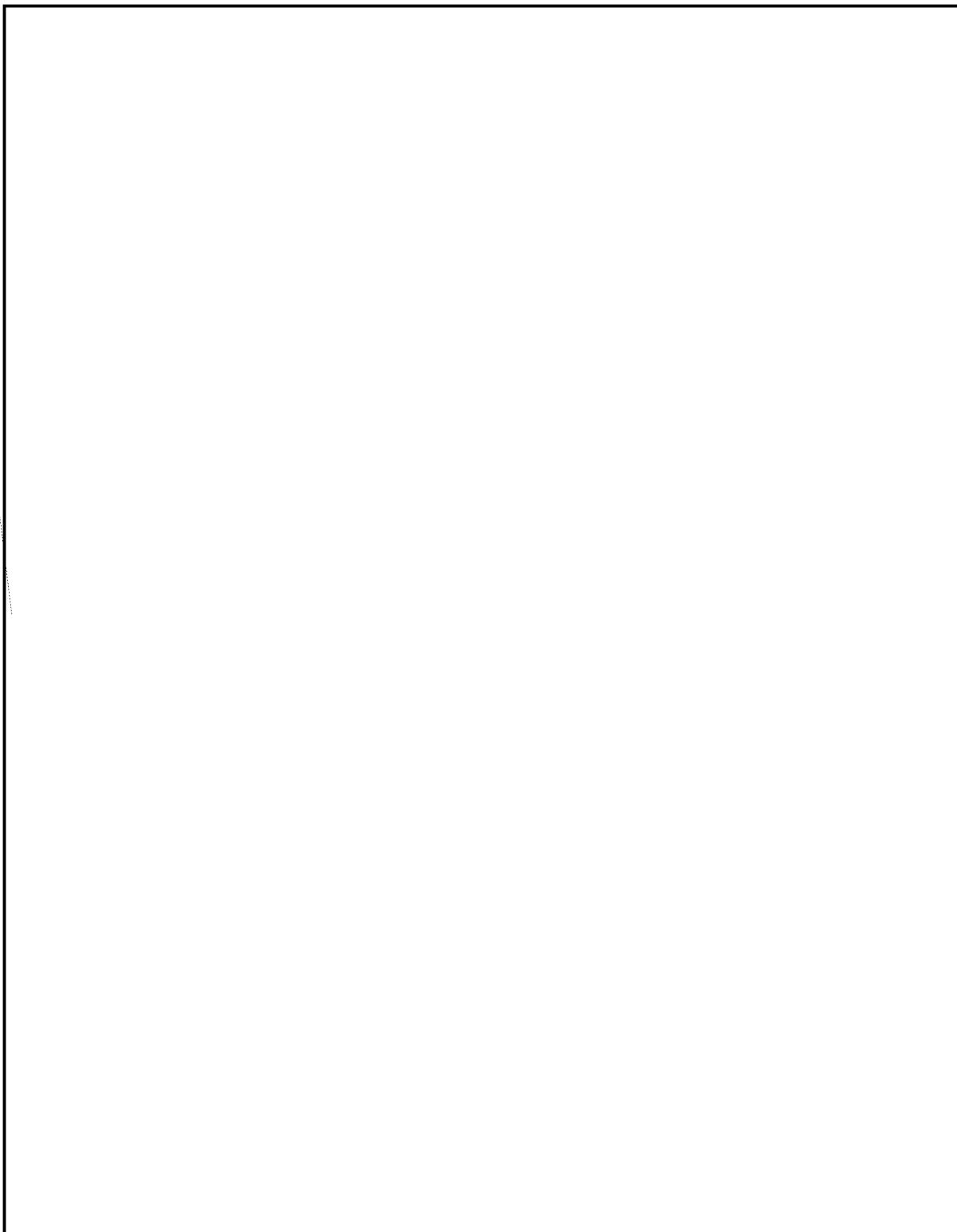
~~SECRET~~

~~SECRET~~
CI THREAT PROGRAM GUIDE

b1
b7E

OVERVIEW

(S)



~~SECRET~~

~~SECRET~~
CI [] THREAT PROGRAM GUIDE

INTRODUCTION

b7E

(U) This CI [] *Threat Program Guidance* offers a template for field offices to focus their efforts and limited resources against the “most threatening” foreign [] collectors []
[]

(U) The guidance is presented in two parts:

(U) *Part I—Managing the [] Threat* provides an overview of what the successful [] threat program looks like from a *Program Manager(PM)/ASAC’s perspective*, what are the Program Manager’s responsibilities, and what results the Program Manager should expect to achieve if the CI Program is managed in a professional, sophisticated, and focused manner.

b7E

(U) *Part II—SSA Core Activities* presents a more detailed description of *specific activities an SSA should use* in the day-to-day execution of the program []
[]

~~SECRET~~

~~SECRET~~

PART I: MANAGING THE [REDACTED] THREAT PROGRAM

b7E

(U) The PM/ASAC is responsible for ensuring that the CI Program within the division achieves each of the five program activities outlined on page one. The PM/ASAC is also responsible for the professional and consistent execution of the *Core Activities* identified in *Part II* of this guidance.

(U) The success of the [REDACTED] Threat Program depends on collaborative relationships with both external and internal partners. Because Program success is dependent on collaborative relationships, the PM/ASAC is responsible for ensuring such relationships are established and sustained and contribute to Program Objectives.

b7E

(U) Finally, *Part I* describes the anticipated results of these activities from a program management perspective.

➤ [REDACTED]

b7E

Expected Program Performance

(S)

b1
b7E

ANTICIPATED RESULTS:

(S)

b1
b7E

~~SECRET~~

~~SECRET~~
CI [] THREAT PROGRAM GUIDE

b7E

Expected Program Performance

b1
b7E

(S)

ANTICIPATED RESULTS:

(S)

b1
b7E

~~SECRET~~
CI [] THREAT PROGRAM GUIDE

b1
b7E

(S)

b7E

Expected Program Performance

(S)

b1
b7E

ANTICIPATED RESULTS:

(S)

b1

(S)

b1
.b7E

b7E

Expected Program Performance

(S)

b1
b7E

ANTICIPATED RESULTS:

(S)

b1
b7E

(S)

b1
b7E

b7E

Expected Program Performance

(S)

b1
b7E

ANTICIPATED RESULTS

(S)

b1
b7E

~~SECRET~~
CI THREAT PROGRAM GUIDE

PART II. CORE ACTIVITIES FOR THE CI SSA

(S)

b1
b7E

b7E

(S)

--

b1
b7E

(S)



b1
b7E

Best Practices:

SSAs should consider whether the following *Best Practices* are appropriate for their field office program:

(S)

-
-

b1
b7E

~~SECRET~~
CI [REDACTED] THREAT PROGRAM GUIDE

[REDACTED]

b7E

(S)

[REDACTED]

b1
b7E

Best Practices:

(S)

[REDACTED]

b1
b7E

[REDACTED]

b7E

(S)

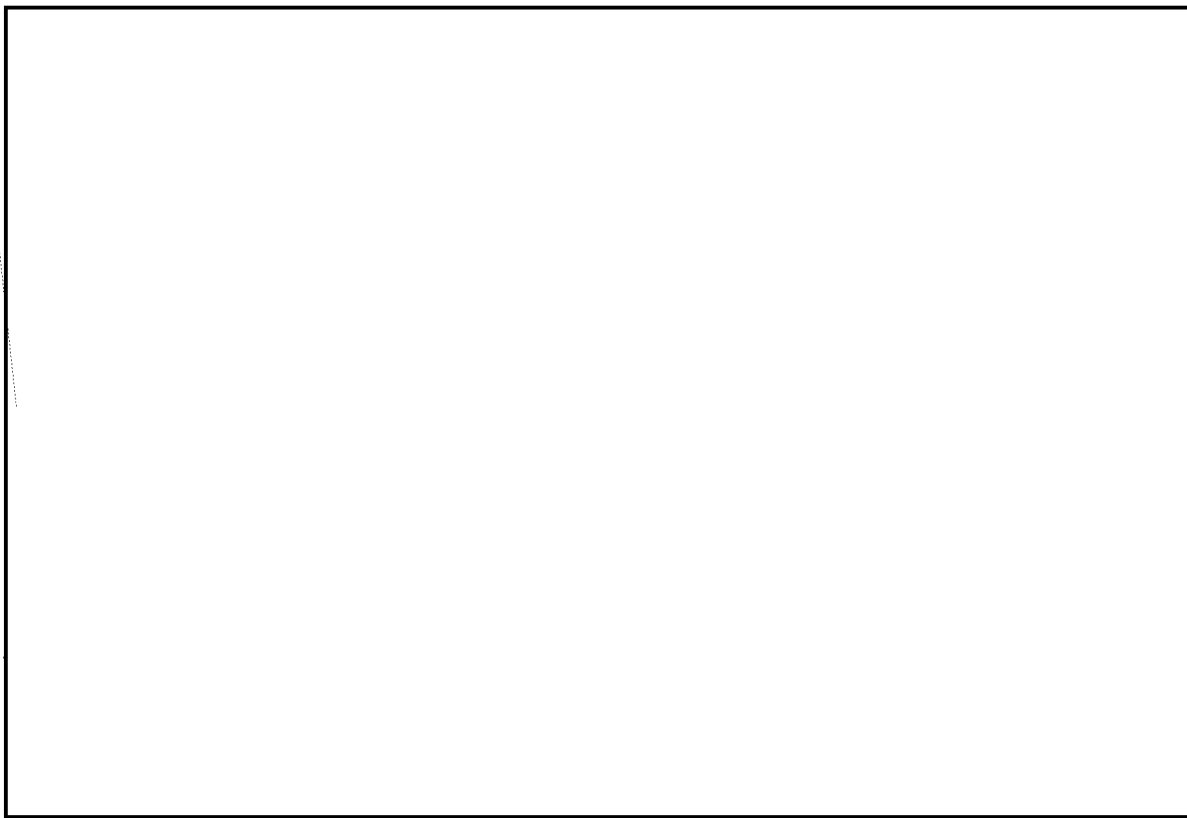
[REDACTED]

b1
b7E

~~SECRET~~

CI THREAT PROGRAM GUIDE

(S)



b1
b7E

Best Practices:

(S)



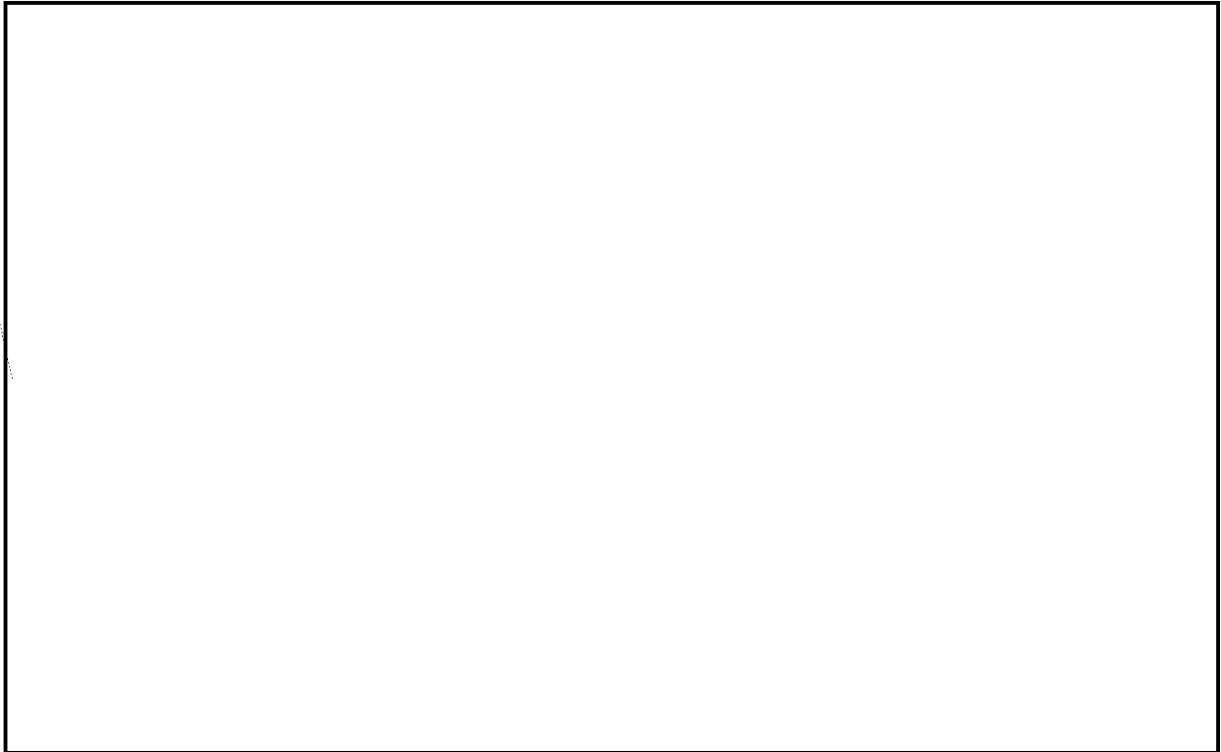
b1
b7E

~~SECRET~~
CI [] THREAT PROGRAM GUIDE

➤ []

b7E

(S)



b1
b7E

Best Practices:

(S)



b1
b7E

(S)



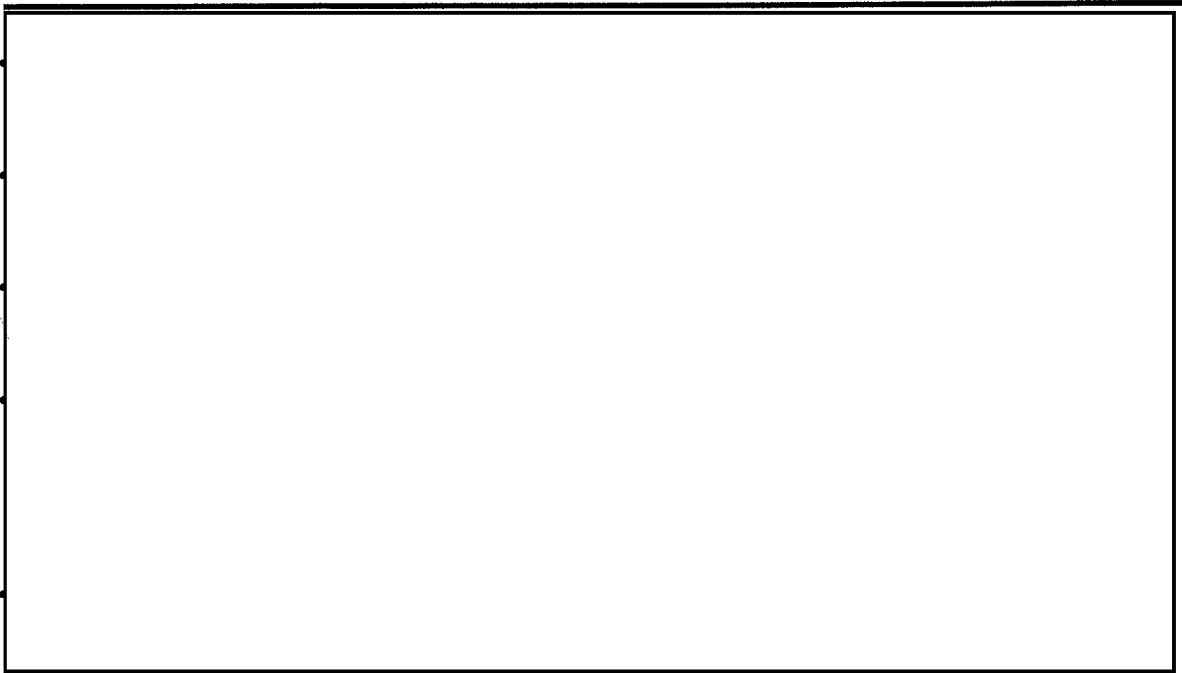
b7E



b1
b7E

~~SECRET~~
CI THREAT PROGRAM GUIDE

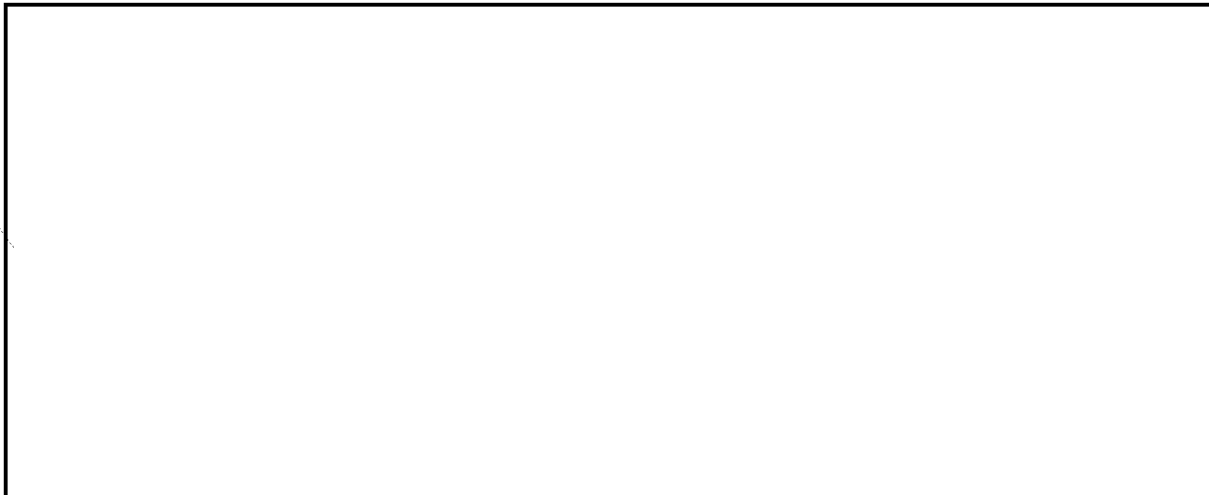
(S)



b1
b7E

Best Practices:

(S)



b1
b7E

Counterintelligence [redacted] Threat Program

Identify the [redacted] threat

b7E

(S)

~~SECRET~~

b1
b7E

Core Elements Reference Guide

b7E

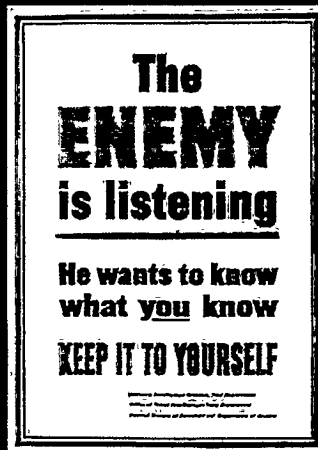
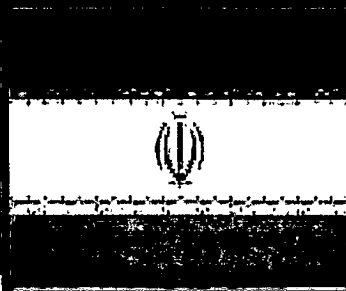
(S)

b1
b7E

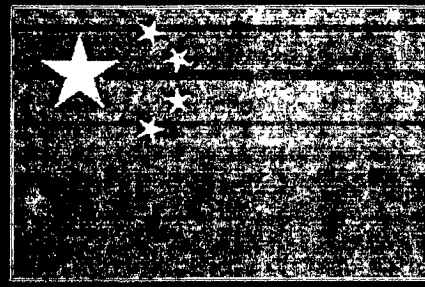
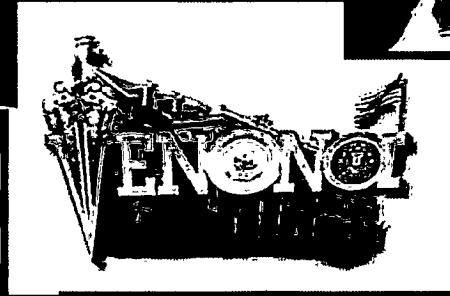
II



The FBI's Counterintelligence Program



b6
b7C

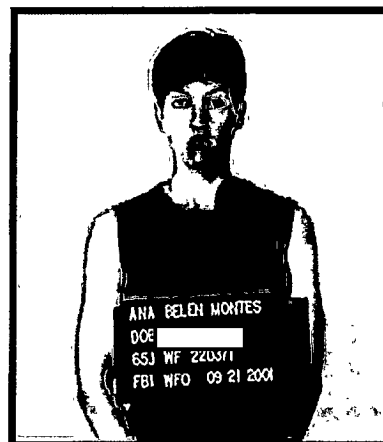
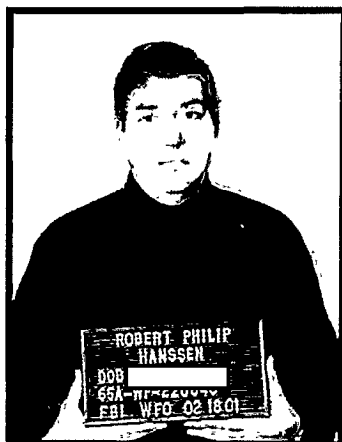




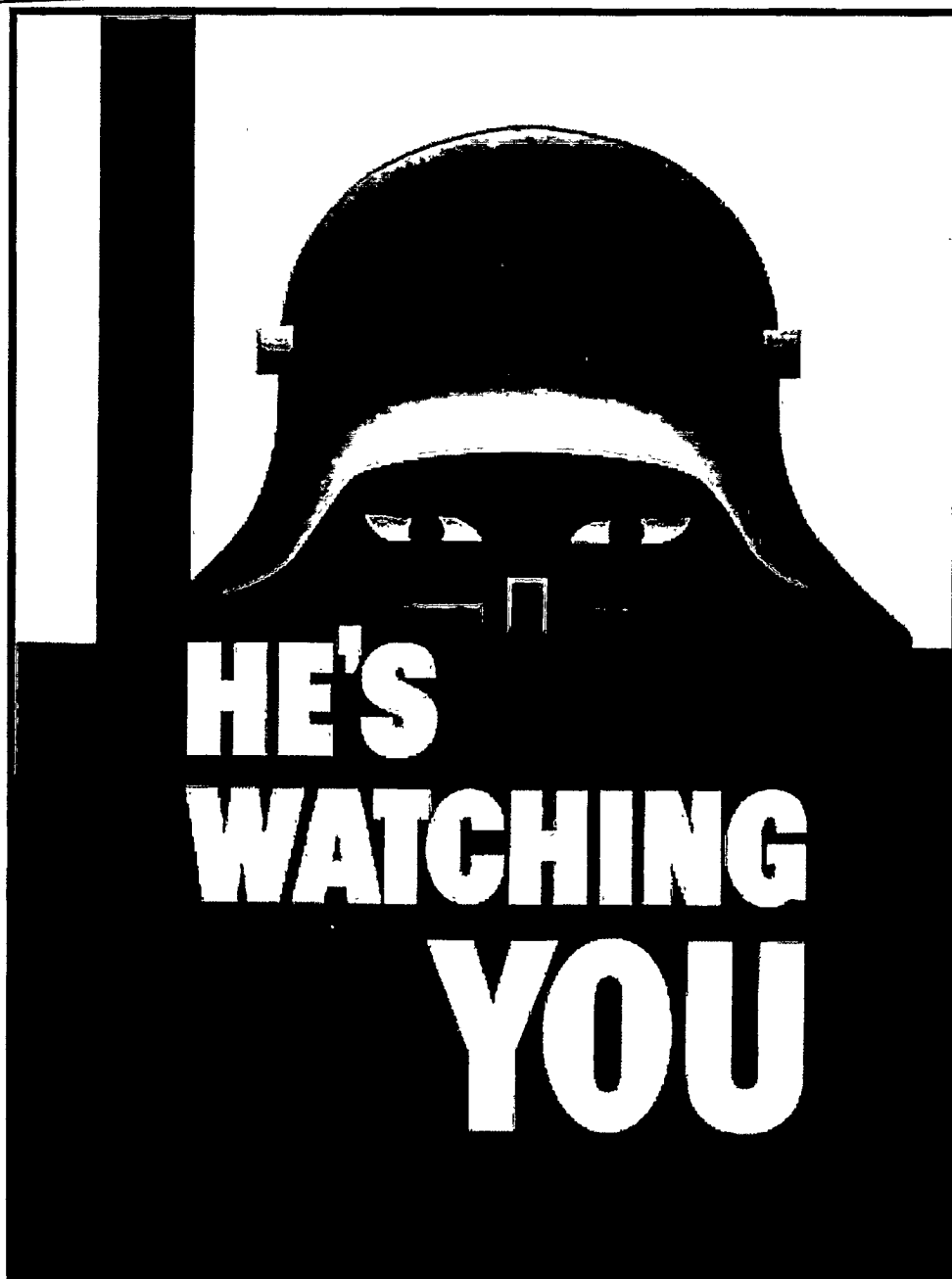
Introduction

The Federal Bureau of Investigation (FBI) is charged with a mission of vital importance to the national security of the United States, that of protecting the nation from threats posed by the activities and assets of foreign intelligence services (FIS). The intelligence services of our adversaries are dedicated to using all means at their disposal to obtain sensitive information which enhances the strategic position of their country while disadvantaging the United States. Countering this activity is one of the top priorities of the FBI. As the lead agency for counterintelligence (CI) in the United States, and the primary investigative component of the U.S. Department of Justice, the FBI has the responsibility to oversee the integration of U.S. law enforcement and intelligence efforts to ensure all available means are brought to bear to mitigate the ongoing and daunting threat of FIS. The Counterintelligence Division (CD) provides centralized management and oversight for all FBI CI investigations, and establishes the strategy for the CI Program.

The FBI has combated FIS activity in the United States for many years. The last decade saw the collapse of the Soviet Union and vaunted KGB and other intelligence services of the Warsaw Pact. These historical changes did not diminish the threat posed to our national security by FIS. The arrests and successful prosecutions of spies, such as former FBI supervisory special agent Robert Hanssen, National Reconnaissance Office contractor Brian Regan, and Defense Intelligence Agency (DIA) analyst Ana Montes clearly demonstrate that the successor services of our Cold War adversaries still seek our secrets.



b6
b7C



The FBI and Counterintelligence

The FBI is not new to CI work. The fact is the Bureau has been conducting investigations in this field for about 100 years. The FBI can trace its origins back to 1908 with the establishment of a small, unnamed "special agent force" located within the U.S. Department of Justice. In 1909, it became known as the Bureau of Investigations (BOI). During the First World War, the United States suddenly found itself to be the target of foreign saboteurs and spies. In 1917, Congress passed the Espionage Act to counter this activity, and the Bureau was tasked with enforcing the Act. During the 1920s and 1930s, the BOI CI responsibilities increased as the threat posed from communist and fascist governments grew. In the early 1930s, the BOI was renamed the Division of Investigation to reflect its growing responsibilities. In 1935, President Franklin D. Roosevelt signed legislation that officially recognized the Division as the Federal Bureau of Investigation.

Under the directorship of J. Edgar Hoover, the FBI's CI mission became more focused. As the 1930s progressed, Nazi Germany's and Imperial Japan's aggressive foreign policies of expansion and world dominance were exposed to the world. Recognizing this grave threat, President Franklin Roosevelt signed an executive order in 1939 that gave the FBI investigative authority for espionage, counterespionage, sabotage matters, subversive activities, and violations of the neutrality laws.

As another World War erupted in Europe in 1939, the FBI again found itself in conflict with foreign spies. In 1941, the FBI mounted a proactive and very successful double agent operation that led to the arrest of dozens of Nazi agents which crippled German Intelligence activity in the United States. On December 7, 1941, the United States entered the War when the Japanese attacked the U.S. Fleet at Pearl Harbor, Hawaii. The FBI's CI efforts intensified and investigations led to the arrest of both Japanese and German agents in the United States. As the War progressed, the importance of the FBI's neutralization of German Intelligence operations in 1941 became apparent as the Nazis attempted to land saboteurs by submarine in 1942. Robbed of any support mechanism in the continental United States, two teams of German saboteurs who landed on beaches in Long Island, New York, and Florida were quickly apprehended by the FBI. All eight saboteurs, who had landed in late June 1942, were arrested within two weeks. They were tried by a US Military tribunal in Washington, D.C., in July, and six of the eight were sentenced to death (two received prison sentences). The executions were carried out during the first week of August 1942.

Following the end of World War II in 1945, U.S. policymakers were able to assess the performance of the country's intelligence services. This led to the passage of the National Security Act of 1947. The Act established the foundation for today's U.S. Intelligence Community (USIC) and created the Central Intelligence Agency (CIA), U.S. Air Force, and the National Security Council.



The end of World War II also marked the termination of the alliance between the West and the Soviet Union. Former allies now became adversaries in what came to be known as the *Cold War* began. The Soviet intelligence services (SIS) became the primary foes of U.S. CI agencies, although the FBI was already aware that Soviet Intelligence had been aggressively pursuing American secrets for many years. U.S. CI operations, like VENONA, described below, disclosed how active the SIS were in the United States.

On February 1, 1943, the U.S. Army's Signal Intelligence Service, a forerunner of the National Security Agency, began a small and very secret program, codenamed VENONA. The original objective of the VENONA program was to examine, and possibly exploit, encrypted Soviet diplomatic communications. It took almost two years to break the Soviet code. American analysts discovered that the Soviet communications dealt with not only diplomatic subjects, but also espionage. The information was provided to the FBI, and led to the opening of many CI investigations. VENONA is most famous for exposing Julius (codenamed LIBERAL) and Ethel Rosenberg, and helped give indisputable evidence of their involvement with Soviet Intelligence efforts to obtain the secrets of the Atomic Bomb.

The late 1940s and early 1950s were marked by well-publicized Congressional hearings into Soviet penetrations of various U.S. government (USG) agencies, such as the U.S. Departments of State and Defense. It was during this time frame that the U.S. Congress passed the Internal Security Act of 1950, which established the statutes used today to investigate unauthorized disclosure of classified information by USG employees.

The Cold War spanned over four decades and spies played an integral role in the hostilities. During this period, the FBI not only contended with Soviet and Chinese spies, but also with those of the "satellite" countries of the Warsaw Pact (e.g., Poland, Czechoslovakia, East Germany, etc.).

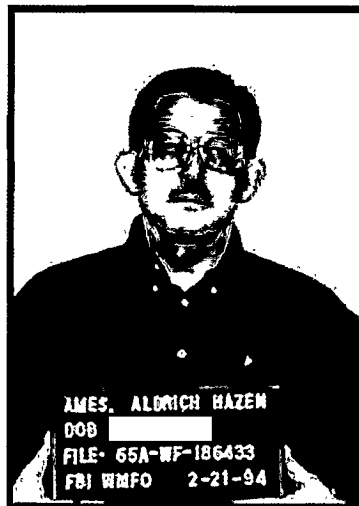
As the Cold War intensified and fears of the spread of communism in U.S. society mounted, the FBI expanded its internal investigations of groups and individuals viewed to be a threat to national security. It was during this period that the FBI launched COINTELPRO (or Counterintelligence Program). By the late 1960s, America was deeply immersed in the Vietnam War, and the growing civil unrest and mass demonstrations served to fuel USG concerns and fears that these elements posed to national security threats. COINTELPRO mirrored this concern and by the late 1960s, the program had become heavily engaged in aggressive domestic operations which included wiretaps, "black bag" entries of homes and businesses, personal "smear" campaigns, and extensive record keeping on American citizens.

The FBI terminated COINTELPRO in the early 1970s, and the FBI internal security and CI efforts soon came under scrutiny by the U.S. Congress. The Congressional hearings and commissions that followed, including the Church Committee, led to the passage of key legislation and guidelines which had great impact on the USIC and the FBI's CI work. In May 1976, the National Security Investigations Guidelines (or Attorney

General Guidelines) were issued. These guidelines defined "national security" matters and required investigations have some connection to a foreign power. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA) which established the FISA Court and procedures to obtain electronic surveillance in national security cases.

Although many FBI investigations during the 1960s and early 1970s focused on domestic groups, the FBI had continued to conduct CI investigations of FIS. FIS remained very active in the United States during this time frame. The 1980s saw a revitalized CI Program focused primarily on the activities of FIS of communist countries. Dozens of arrests were made of FIS agents and intelligence officers (IOs) who attempted to collect primarily classified military, technical, and political information that would allow Communist countries to gain an edge in weapons development, expand/enhance their influence in other countries, and win an actual shooting war should one break-out with the West. This reached a high point in 1985 (also called the *Year of the Spy*), when the FBI arrested 15 spies.

The fall of the Berlin Wall marked the end of the Cold War and saw the dissolution of the Soviet Union and the Warsaw Pact. Many adversarial FIS also ceased to exist. However some of these were soon reconstituted with very capable organizations. The new Russian Foreign Intelligence Service (SVR) replaced the now defunct KGB (the civilian intelligence service of the Soviet Union), and continued to run aggressive operations in the United States. In some instances, the SVR continued to use agents who had been operated by the KGB. For example, in 1994, the FBI arrested a CIA case officer named Aldrich Ames. He had begun his espionage career with the KGB in 1985 and was inherited and operated as an agent by the new SVR in the early 1990s.



b6
b7C

The FBI encountered new adversaries in the post-Cold War era as CI investigations disclosed efforts by countries, long considered to be our allies, engaged in intelligence operations in the United States. Additionally, the Cold War was replaced by a new type of conflict, an economic war. U.S. economic intelligence and trade secrets became primary targets of FIS. Congress passed the Economic Espionage Act of 1996 to counter the attempts of foreign adversaries to target and acquire U.S. economic secrets.

The horrific events of September 11, 2001, led to heightened concerns. New legislation was passed which had a significant impact on the USIC and the FBI's CI Program. The Patriot Act of 2001 removed many legal barriers that had prevented law enforcement, intelligence, and national defense communities from sharing information and coordinating their work to protect U.S. national security (e.g., prosecutors could now share evidence obtained through grand juries with intelligence officials and intelligence information could now be shared more easily with Federal prosecutors).

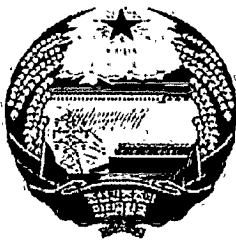
Subsequently, President George Bush signed the Intelligence Reform and Terrorism Prevention Act of 2004 which created the position of Director of National Intelligence (DNI). The act redesigned how the USIC was administered and led to the establishment of the National Security Branch (NSB) of the FBI. Today, the NSB oversees the national security operations of the FBI's CD, Counterterrorism Division, Directorate of Intelligence (DI), and Weapons of Mass Destruction (WMD) Directorate.

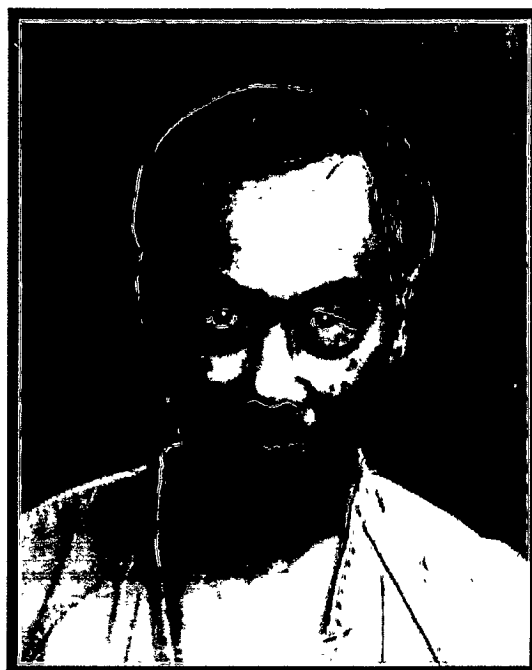


President George Bush signs the Intelligence Reform and Terrorism Prevention Act of 2004

The Threat

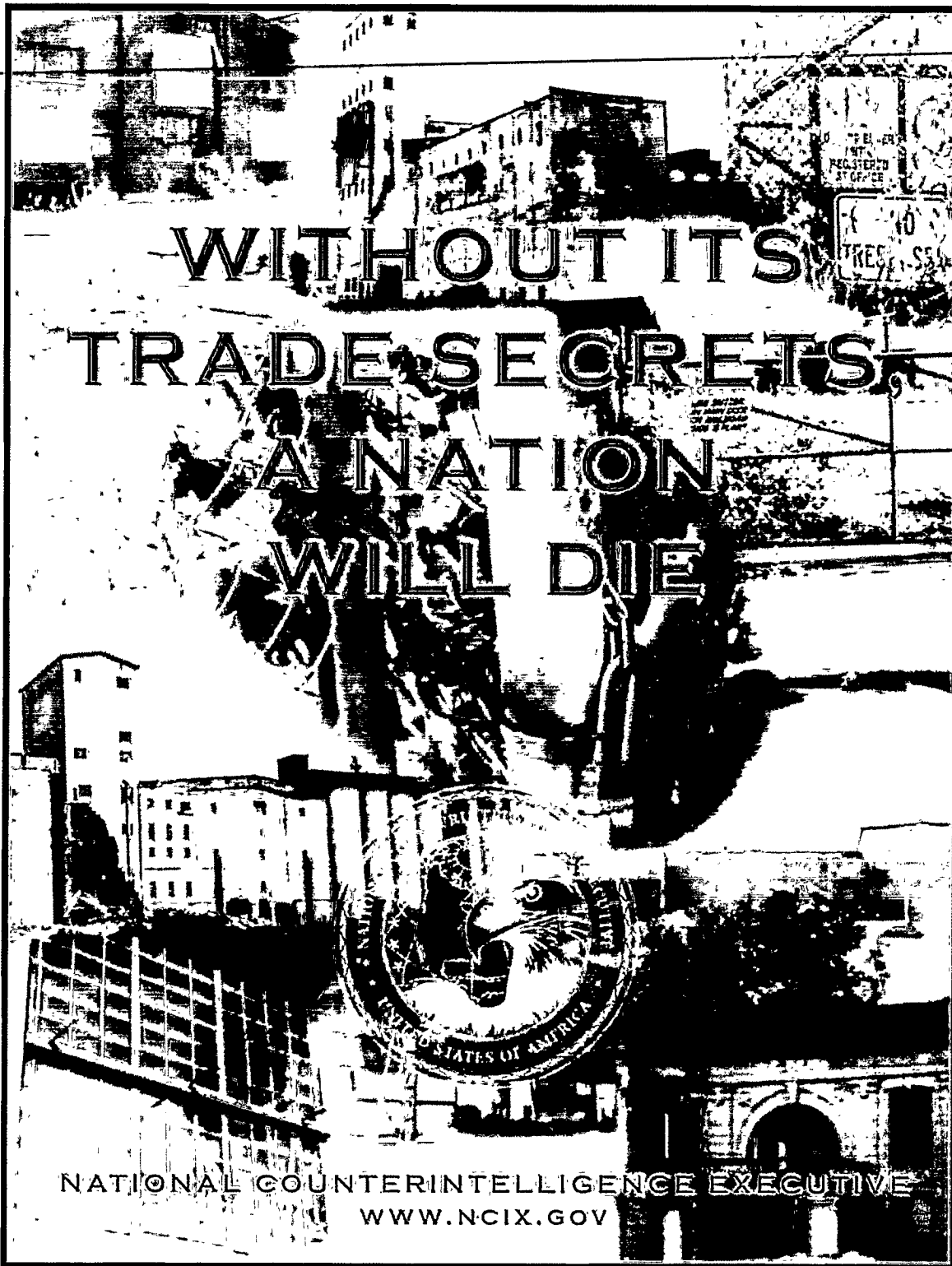
The foreign intelligence threat currently facing the United States from its adversaries is complex and unrelenting. U.S. national security is gravely threatened by FIS and their agents. Foreign adversaries are using every means at their disposal to acquire information and technology in order to gain political, military, and economic advantage over the United States. They attempt to recruit or exploit people in nearly every profession and every "walk of life" to achieve their objectives: USG employees, U.S. military personnel, businessmen, scientists, students, diplomats, and delegations. U.S. firms, universities, national laboratories, and sensitive USG facilities employ and/or interact with foreign nationals locally, nationally, and internationally on a daily basis. These foreign nationals come with skills, services, and products that in an increasingly "globalized world," have become integral to U.S. innovation and science and technology leadership. For the most part, such foreign nationals are studying, working, or otherwise engaging in legitimate activities, yet foreign adversaries can and frequently do use these groups as cover to covertly acquire or illegally transfer U.S. information and/or technology, including proprietary information and trade secrets. Their collection efforts target nearly every entity involved in classified and unclassified work throughout the United States, including not only USG entities, but large and small businesses, from the multi-national corporation to the "mom and pop" subcontractor who possess or have access to sensitive trade secrets. Foreign adversaries also target academia, from the large state university to the small private college, and research laboratories, from the national laboratory to the small independent research institute, in order to obtain sensitive information.





Chi Mak

On May 9, 2007, a jury in the U.S. District Court for the Central District of California convicted Chi Mak, an engineer for the Anaheim, California-based naval defense contractor Power Paragon. Mak was convicted of conspiring to export U.S. defense technology to China, acting as an unregistered foreign agent, attempting to violate export control laws, and making false statements to the FBI. The FBI's Los Angeles Division arrested Mak and his wife, Rebecca Chiu, in October 2005 following the discovery of encrypted compact discs which contained documents on submarine propulsion systems, solid-state power switches for Navy vessels, and information on future military electronic systems. The compact discs were found in the luggage of Mak's brother and sister-in-law as they boarded a flight to Hong Kong. Mak, the principal engineer for the U.S. Navy's Quiet Electric Drive (QED) propulsion system, worked on more than 200 defense and military projects during his career. Following Mak's conviction, four of his family members pleaded guilty to related charges.



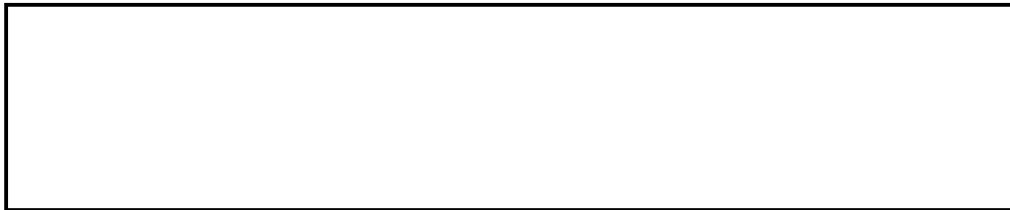
Economic Espionage

U.S. economic and trade secrets are priority targets of foreign adversaries. U.S. private sector studies estimate losses in the billions of dollars every year. However, the extent is difficult to ascertain because U.S. industry is sometimes reluctant to report losses. The Economic Espionage Act (EEA) imparted criminal liability for the theft or misappropriation of trade secrets as well as any attempt or conspiracy to steal or misappropriate trade secrets. Prior to passage of the EEA, there were very few legal options available to Federal prosecutors to protect intellectual property rights of these assets. The few federal laws that did touch upon trade secret theft were not broad enough to reach the kinds of theft being perpetrated, or strong enough to adequately punish this activity. In addition, significant variations remained in the ways trade secret laws had developed at the state level. The civil remedies provided by these state laws were often inadequate in compensating a business for the theft of its trade secrets.

How do foreign adversaries collect U.S. economic and trade secrets? Listed below are some overt and covert methods that they use.

Overt Methods:

-
-
-
-



b7E

Covert Methods:

-
-
-
-
-



b7E

What are foreign adversaries attempting to collect in the United States? The following technologies are some of their priority targets:

-
-
-
-
-
-
-
-
-



b7E

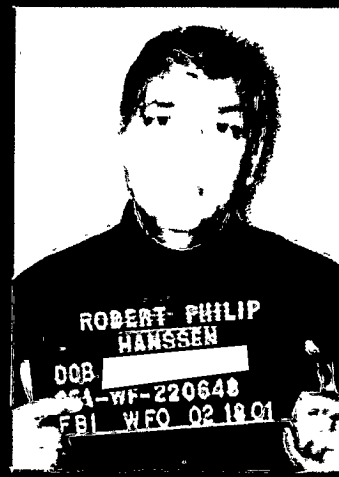


THE OATH

...solemnly swear that I will support and defend the Constitution of the United States...bear true faith and allegiance...will well and faithfully discharge the duties of the office...So help me God.

ESPIONAGE

The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.



b6
b7C

Robert P. Hanssen
Spy • Traitor • Deceiver

Office of the National Counterintelligence Executive

www.ncix.gov

Countering the Threat

Strategy

The FBI's Counterintelligence Division ensures that offensive operations and investigations are fully coordinated with the USIC and are focused on those countries, foreign powers, or entities which pose the most significant threat to the United States.

The strategic goals of the CI Program are to:

♦ Prevent the proliferation of weapons of mass destruction, its delivery systems, and technology.

Of all the threats facing the United States today, the most significant is the potential for an agent of a hostile group or foreign nation to enhance the capability of a nation to produce or use WMD. This threat specifically applies to hot spots throughout the world in which the United States has significant national security interests, and to which worldwide destabilization could result. The CI Program considers this its top priority. The FBI works to fulfill this important responsibility by [REDACTED]

b7E

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

The unfortunate experiences of recent years clearly demonstrate the critical importance of preventing FIS attempts to penetrate the USIC. The FBI accomplishes this by [REDACTED]

b7E

The USG also supports research and development in a large number of agencies, in numerous locations, involving the use of thousands of USG contractors. The FBI has the responsibility to assess the threat against these projects and to initiate operations that are directed at countering the threat. The FBI works extensively with the USIC to facilitate this important mission. USG entities, principally the U.S. Departments of Energy and Defense, constitute the primary focus of FBI activity in this area.



b6
b7c

"There is one I dread,
and that is, their
I could, therefore,
the most attentive be kept..."

George Washington

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE • WWW.NCIX.GOV

◆ Prevent the loss or compromise of Critical National Assets and critical U.S. information and technology.

Critical National Assets (CNAs) are government and private sector policies, information, technologies, and industries (e.g., nuclear power plants, telecommunication systems, major banking and financial computer networks, etc.) that, if acquired, modified, or manipulated by our adversaries would seriously disadvantage U.S. national and economic security. The FBI has a major role in identifying threats against these assets and assessing their vulnerability. The FBI works closely with other members of the USIC and with the private sector to accomplish this mission.

◆ Enhance the national threat picture by responding to National Intelligence Priorities Framework and other collection requirements.

The FBI CI Program recognizes the importance of planning for and responding to the intelligence needs of the NSB, Office of the Director of National Intelligence (ODNI), and other CI requirements in the Executive Branch. Responding to these “needs” requires the CI Program have the flexibility to respond to new and developing threats, as well as to initiate foreign positive intelligence collection operations that respond to high priority national requirements as part of its day-to-day operations.

The CI Program works to ensure:

-
-
-



b7E

**X-Rays Can't Show
Espionage Indicators.**

POWER
GREED DEBT
REVENGE
EXCITEMENT
OPPORTUNITY

**Proactive Counterintelligence
& Security Programs Can.**

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE
www.ncix.gov

Implementing the Strategy

The CI Program achieves its goals by:

♦ Engaging in strategic partnerships.

Regardless of how many resources the FBI commits to its CI Program, it cannot protect the entire realm of U.S. political, military, economic, and technologic information from foreign exploitation and compromise. To be successful, the FBI enlists the USIC and the wider USG community to aid in reducing the effectiveness of foreign intelligence collection efforts. By leveraging these two communities' expertise, authorities, and resources and, in return, making available to them FBI assistance, a formidable multi-agency team is assembled to protect U.S. national security interests.

♦ Identifying foreign intelligence collection, objectives, officers, agents, and operations.

Since the FBI began working counterintelligence cases many years ago, it has strived to identify FIS collection targets, personnel and agents, operations, and methodology as a means to counter and neutralize foreign intelligence activity in the United States. This has been accomplished through the use of proactive and sophisticated operations [REDACTED]

b7E

[REDACTED] FBI analysts play a key role in assessing FIS targeting priorities and capabilities, as well as identifying effective countermeasures that can be employed to combat foreign intelligence efforts.

b7E

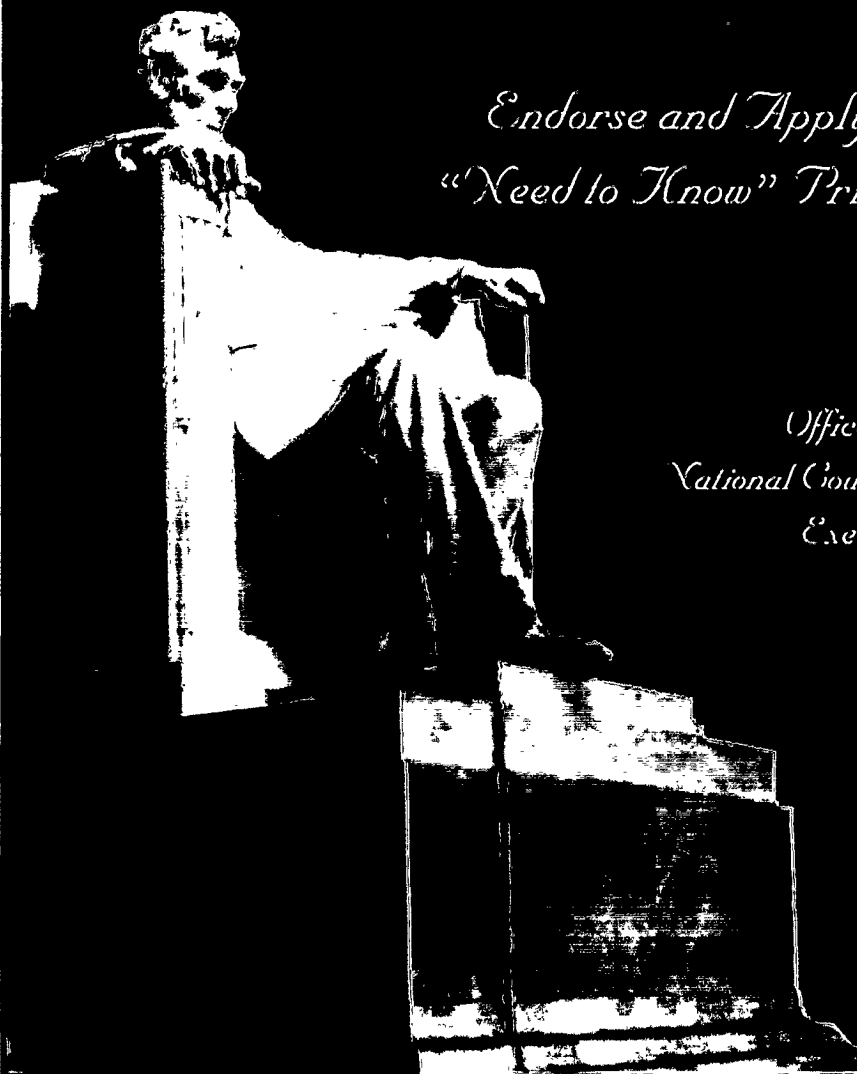
♦ Detecting, disrupting, and deterring the *insider threat*.

Every major espionage case over the past 15 years has involved an "insider" who betrayed their employer for money, revenge, or (in one instance) ideology. The trusted insider turned traitor has proven to be the most effective tool available to FIS in penetrating the most sensitive and highly protected agencies of the USG. It can be

America will never be destroyed from the outside.

*If we falter and lose our freedoms,
it will be because we destroyed ourselves.*

— Abraham Lincoln



*Endorse and Apply the
“Need to Know” Principle.*

*Office of the
National Counterintelligence
Executive*



www.nce.gov

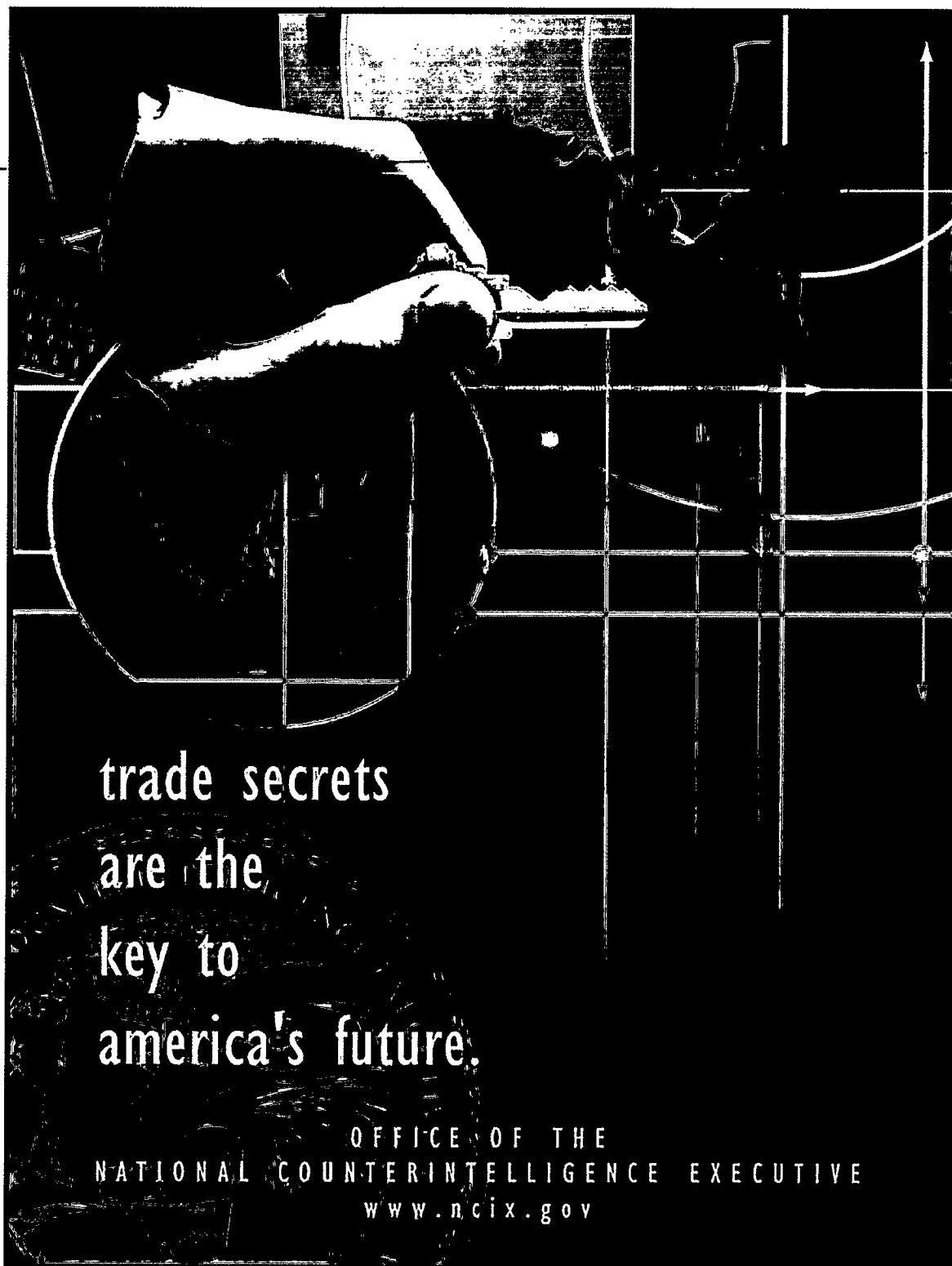
expected that USG personnel will remain a primary target of foreign intelligence collection well into the 21st Century. With globalization and the emphasis by foreign collectors on compromising critical U.S. technologies, employees of USG contractors are equally high-value targets for foreign intelligence collectors. There is no doubt these collectors use the same techniques against U.S. industry as they have found effective against USG agencies, using the trusted insider to steal classified or sensitive information and technologies. To meet this dual challenge, CD has established the National Insider Threat Program. The program is centered on Section 811 of the Intelligence Authorization Act of 1995, which requires USG agencies immediately contact the FBI when it is believed that any information indicating classified information has/is being disclosed to a foreign government without authorization. The primary goals of the program are to ensure USG agencies understand Section 811 and its requirements, and to educate the business and academic sectors about the insider threat.

♦ Fully integrating National Intelligence Requirements into collection efforts.

The CI Program is a collector of foreign intelligence, and has been for many years. Throughout the Cold War, the CI Program collected and disseminated significant amounts of foreign intelligence. Although its contribution advanced USIC intelligence objectives, the collection of this information was by-and-large a reactive collateral activity, collected by field offices as they pursued their CI interests. On occasion, the CI Program would initiate an action to specifically collect positive intelligence, but this was the exception and not the rule. In the wake of the terrorist attacks on 9/11, it was critical the CI Program become more proactive in collecting foreign intelligence. In pursuit of this strategy, the FBI's NSB and its operational components established a comprehensive reporting system to collect and disseminate valuable intelligence to the USIC and policymakers.

Today, the CI Program plays an important role in this effort by ensuring intelligence collected through its operations is identified, assessed, and prepared for distribution to appropriate USG entities in a timely manner. FBI intelligence analysts (IAs) play a major role in this effort. All FBI field offices have IAs, many of whom are assigned to division [REDACTED]

b7E



trade secrets
are the
key to
america's future.

OFFICE OF THE
NATIONAL COUNTERINTELLIGENCE EXECUTIVE
www.ncix.gov

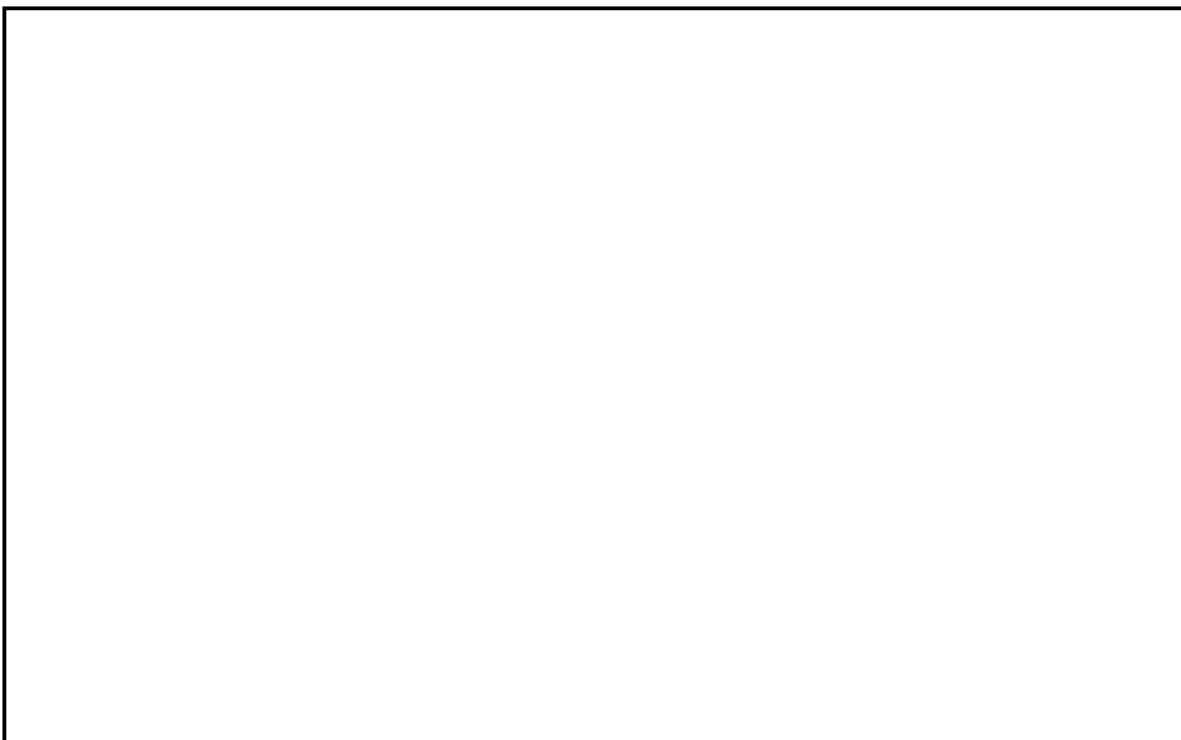
IAs serve as the focal point for the dissemination of CI-related and foreign positive intelligence. [redacted] IAs receive guidance and training from FBIHQ ensuring awareness and understanding of regulations guiding national priorities for intelligence collection, the FBI's role in collection and dissemination of intelligence, and the mechanics of how it should be disseminated.

b7E

IAs are a vital component of the CI Program. Efforts to formalize FBI analysis were initiated in October 1973, as a result of a recommendation by the President's Foreign Intelligence Advisory Board. The FBI initially created a unit to primarily conduct research and analysis of CI matters. This unit was composed entirely of SA personnel. In January 1977, then Director Clarence Kelly approved the idea of creating a cadre of career *Intelligence Research Specialists* (eventually to become known as IAs), allowing the SAs to return to investigative duties. Implementation of the CI Analytical Program also provided a basis of continuity for investigative areas, as SAs characteristically rotated on a two-to-four year cycle.

Since 1977, the CI Analytical Program has grown from [redacted] [redacted] IAs at FBIHQ and field offices. Analysis has become an effective adjunct to the FBI's national security investigative programs with IAs being recognized as experts in their specific geographical, topical, and country disciplines. Additionally, FBI analysts play an essential role in guiding ongoing FBI investigations as well as participating in decision-making, and CI strategic planning at the policy level for both the FBI and the USIC.

b7E



b7E

SECURITY AWARENESS



**Help keep our classified
business ~~secret~~. Don't
discuss classified
information off base.**

EXCERPTED FROM FBI

Academic Alliance

The Academic Alliance is a national outreach effort charged with sharing information and establishing a dialogue with academic institutions to increase awareness of threat and national security issues in order to foster a spirit of cooperation.

The Academic Alliance has two distinct outreach components:

(1) National Security Higher Education Advisory Board

The National Security Higher Education Advisory Board (NSHEAB) includes presidents/chancellors of universities and colleges having the nation's top public and private research institutions. The NSHEAB, which meets regularly, provides a forum for FBI leadership and academia to discuss national security issues of mutual concern. The NSHEAB also facilitates dialogue between USG security officials and academia. The NSHEAB provides the FBI with perspectives on the culture of higher education, including its traditions of openness, academic freedom, and international collaboration.

(2) College and University Security Effort

Through the College and University Security Effort (CAUSE), FBI Special Agents in Charge (SACs) meet with the heads of local colleges and universities to discuss national security issues and share information and ideas. Topics covered include briefings on national security threats that these research institutions may be facing. The FBI enables CI protection by explaining how and why some foreign entities may be attempting to steal research and intellectual property by targeting their academic institutions.

Critical National Asset Initiative

The protection of the nation's most critical national assets has been identified as a priority by the USIC. To that end, the FBI has implemented the CNA Initiative. Through the CNA Initiative, the FBI is committed to leading a coordinated effort with the USIC and other USG agencies to assist in prioritizing those critical technologies, processes, systems, and information that require protection from theft or compromise by foreign adversaries.

*US Constitution — 1st Amendment
Congress shall make no law respecting an
establishment of religion, or prohibiting the free
exercise thereof; or abridging the freedom of
speech, or of the press; or the right of the
people peaceably to assemble, and to petition the
government for a redress of grievances.*

*American freedom includes
a responsibility to
protect US security -
Leaking sensitive
information erodes
this freedom.*

*Office of the
National Counterintelligence Executive
www.ncix.gov*

Counterintelligence Working Groups

(1) National Counterintelligence Working Group

The National Counterintelligence Working Group (NCIWG) was designed to establish strategic interagency partnerships at the senior executive level among the USIC, academia, industry, and defense contractors. Working through the NCIWG, the USIC has conveyed a consistent message with regard to its efforts to protect our national security.

(2) Regional Counterintelligence Working Group

Regional Counterintelligence Working Groups (RCIWGs) are composed of USG CI entities. RCIWGs provide forums to share threat information, identify trends, and discuss strategies, initiatives, and operations.

Summary

Despite the many political, economic, and political changes the United States has experienced during the past century, the threats posed by foreign adversaries and their intelligence components have remained constant. As in the past, FIS continue to seek sensitive information on the USIC, US military, USG political issues, new technological developments, and economic matters. However, their collection methods and priorities are always evolving. The FBI recognizes that a proactive CI strategy is required to counter the FIS threat. The FBI's CI Program collects vital foreign intelligence for the USIC and Government policymakers. It uses analysis to assess the threat and to develop successful countermeasures. Program operations and investigations are geared to disrupt and neutralize FIS collection efforts. Most importantly, the FBI's CI strategy focuses on working not only with other USG agencies, but also with academia, and the private sector. Building and maintaining strong partnerships with all these components are key to effectively countering the FIS threat in the United States and safeguarding national security.

The History of US Counterintelligence – PowerPoint

- Usage period: Circa 2008 to Present

b6
b7c

- Developed by FBI MAPA

- Presentation given at various FBI Intelligence Analysts, New agent Training, and Surveillance Specialists training courses.



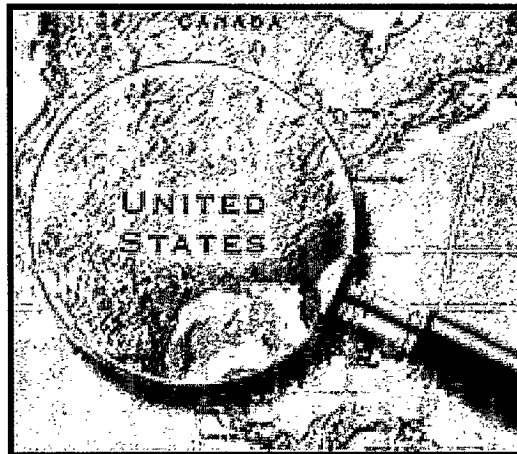
ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-26-2011 BY 65179 DMH/STW

The History of US Counterintelligence





The Importance of an Effective CI Program



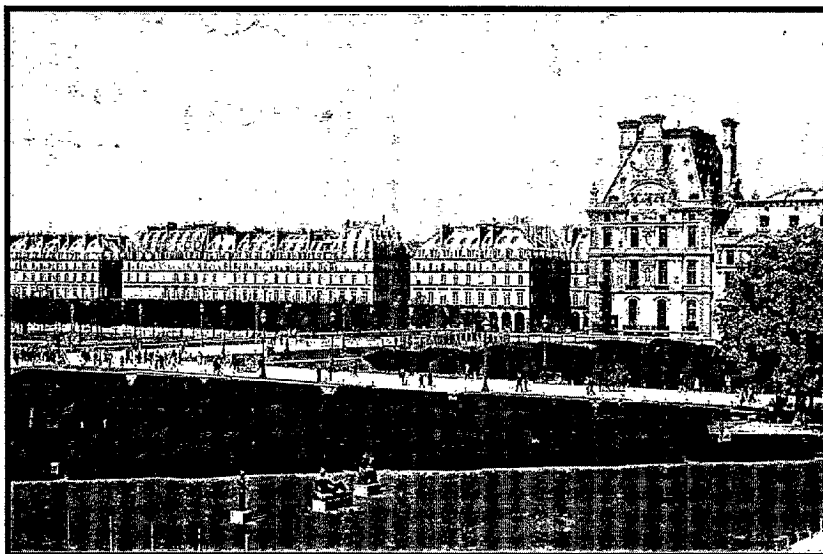
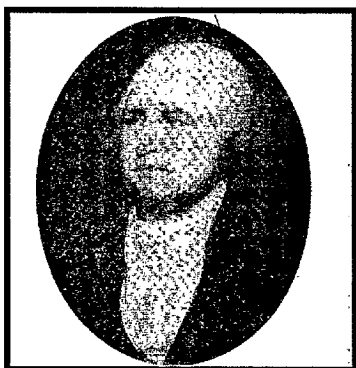


American Revolution: 1776-81





Dr. Edward Bancroft



Jardin des Tuileries
Paris, France



Dr. Edward Bancroft

"In Feb'y 1777, Lord Suffolk formally promised me, in the King's name, a pension of £200 per annum, to commence from the Christmas proceeding. This was for services then rendered and as an inducement to go over and reside in France and continue my services there until the revolt should terminate... His Lordship farther promised that when this should happen (the Revolution end), my permanent pension of £200 would be increased to £500 at least.

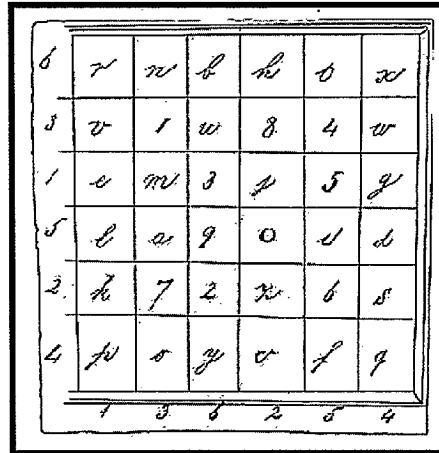
Confiding in this promise, I went to Paris, and in the first year resided in the same house with Dr. (Benjamin) Franklin, Mr. Deane, etc., and regularly informed this government (Great Britain) of every transaction of the American Commissioners and their correspondence with the Secret Committees; of every step and vessel taken to supply the revolted Colonies with artillery, arms, etc.; of every part of their intercourse with the French and other European courts; of the powers and instructions given by Congress to the Commissioners; and when the government of France at length determined openly to support the revolted Colonies, I gave notice of this determination, and of the progress made in forming two Treaties of Alliance and Commerce, and when these were signed on the evening of the 6th of Feb'y, I at my own expense...conveyed this intelligence...to the King's Ministers, within 42 hours from the instant of their signature, a piece of information for which many individuals here would, for purposes of speculation, have given me more than all I have received from (the British) government. Afterwards, when that decisive measure of sending Count d'Estaing with the (French) fleet from Toulon to commence hostilities at the Delaware and New York was adopted, I sent intelligence of the direct object and plan of the expedition..."



Civil War: 1861-65



Union Spy
Elizabeth Van Lew

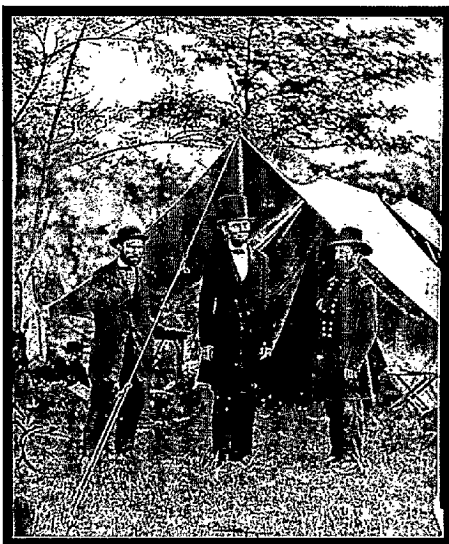


Confederate Spy
Henry Thomas Harrison



Civil War: 1861-65

US Secret Service/National Detective Bureau



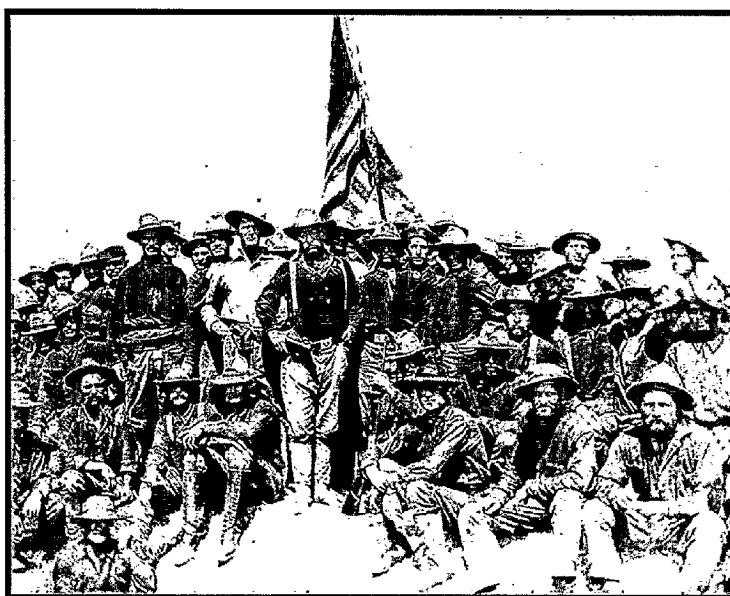
Allan Pinkerton



Lafayette Baker



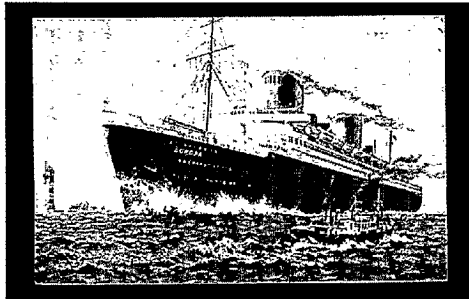
Spanish-American War: 1898





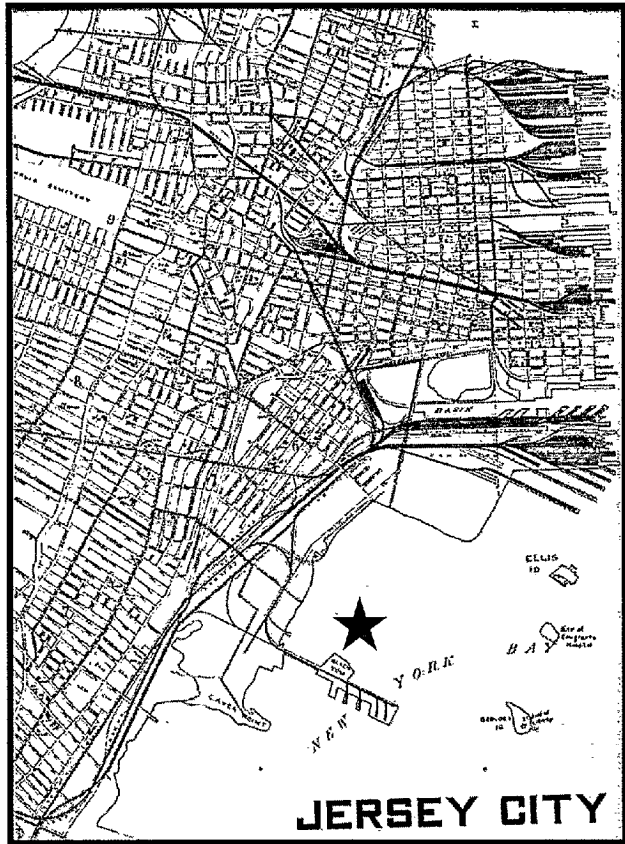
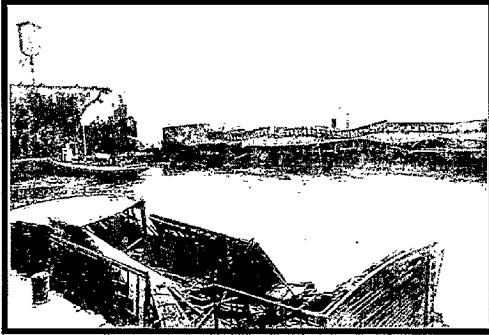
World War I: 1914-18

German Espionage in the United States





Black Tom Island





Espionage Act of 1917



Lt. Lothar Witzke

13-1-18
seofnatugk asiheihbbn uersdausnn
lrseggiesn nkleznsium ehneshaopp
asueasriht hteurmwnsm eaincouasi
insarnvegd esnbtmrcn dtdrzbemmk
kol selzdm auebikbpa taseci sdgt
lhuktnaeie tiebasuera thnoieaen
hsdaaiaim ethmneecd ckdkronesdt

"The bearer of this is a subject of the Empire who travels as a Russian under the name of Pablo Waberski. He is a German secret agent. Please furnish on request protection and assistance; also advance him on demand 1000 pesos of Mexican gold and send his code telegrams to this embassy as official consular dispatches."



Presidential Directive: 1939

President Franklin D. Roosevelt

Directive of the President of the United States, June 26, 1939

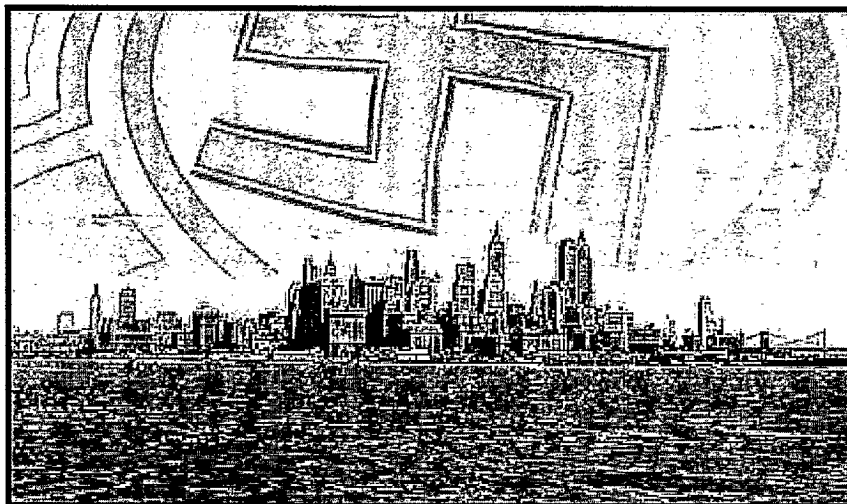
"It is my desire that the investigation of all espionage, counterespionage, and sabotage matters be controlled and handled by the Federal Bureau of Investigation of the Department of Justice, the Military Intelligence Division of the War Department, and the Office of Naval Intelligence of the Navy Department. The directors of these three agencies are to function as a committee to coordinate their activities.

No investigations should be conducted by any investigation agency of the Government into matters involving actually or potentially any espionage, counterespionage, or sabotage, except by the three agencies mentioned above.

I shall be glad if you will instruct the heads of all other investigative agencies than the three named, to refer immediately to the nearest office of the Federal Bureau of Investigation any data, information, or material that may come to their notice bearing directly or indirectly on espionage, counterespionage, or sabotage."



Ritter/Duquesne Espionage Ring





Ritter/Duquesne Espionage Ring



Nikolaus Ritter



b7E



EDMUND CARL WEINE



WALTER BAERCHEN



JOSEF ASEN



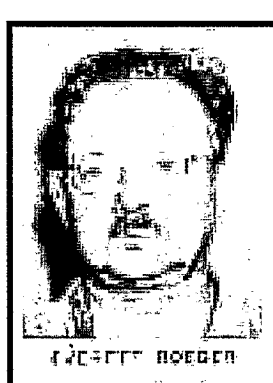
BERNHARD L. LIPP



CARL STORCH



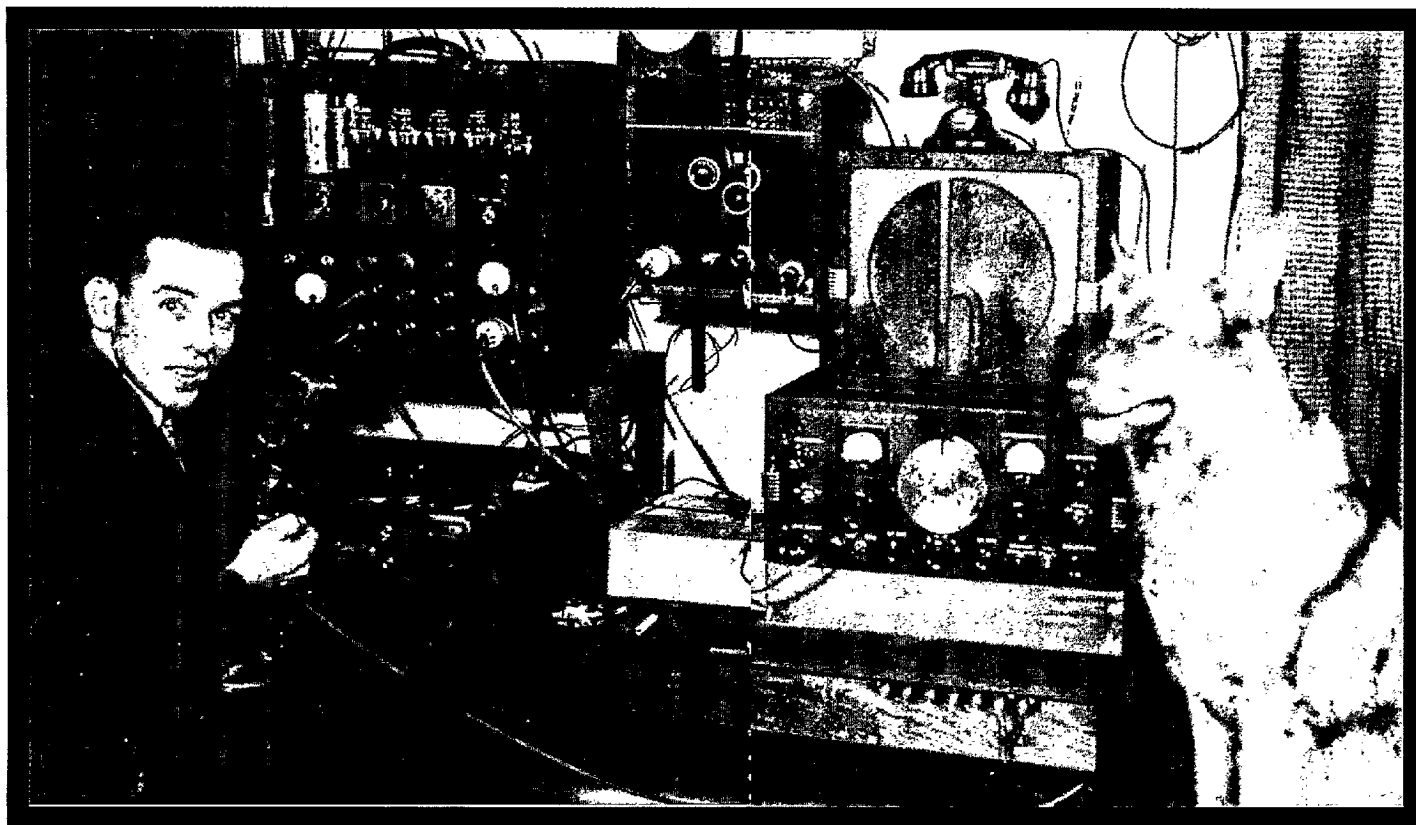
LEO BARKER



GEORGE ROEDER



FRANK JOSEPH STIMLER

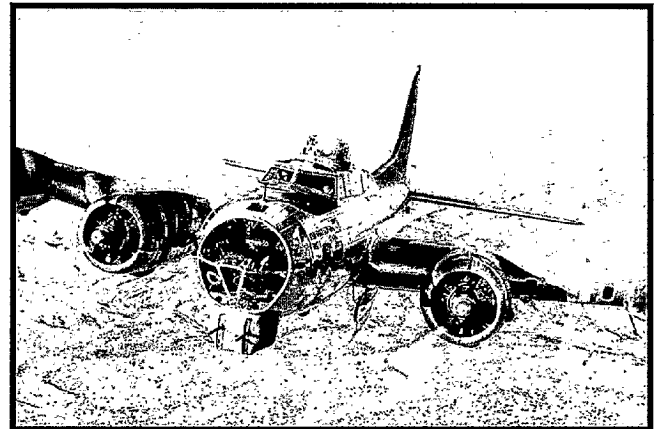
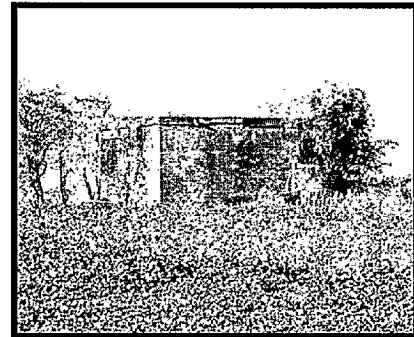
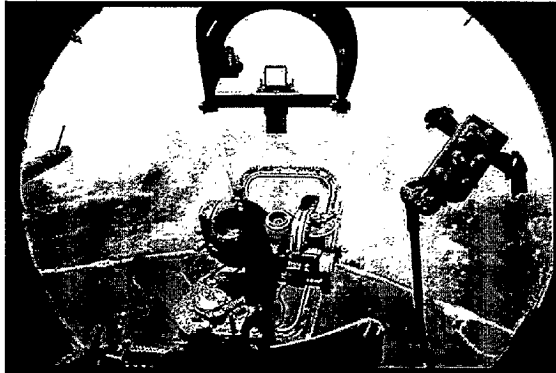


b7E



Norden Bombsight

Ritter/Duquesne Espionage Ring





Norden Bombsight

Ritter/Duquesne Espionage Ring



b7E



b7E

William Sebold: [REDACTED]
Ritter/Duquesne Espionage Ring





b7E

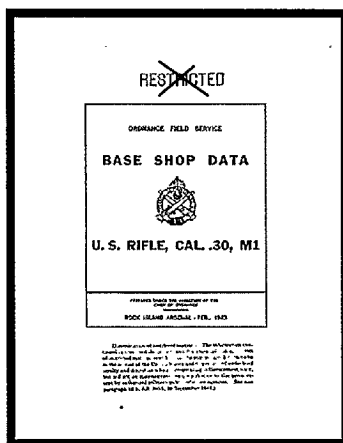
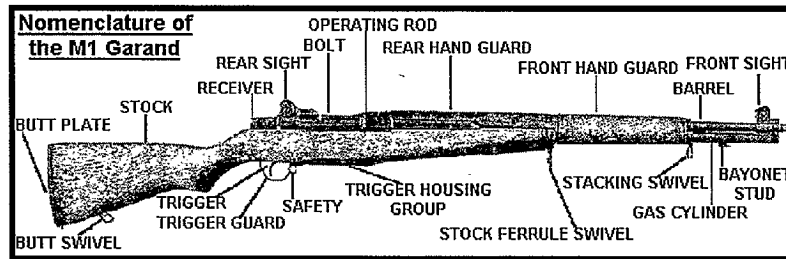
William Sebald, meets
with German agent, Herman Lang,
in New York City.



William Sebold:

M1 Garand Rifle

b7E





Ritter/Duquesne Espionage Ring



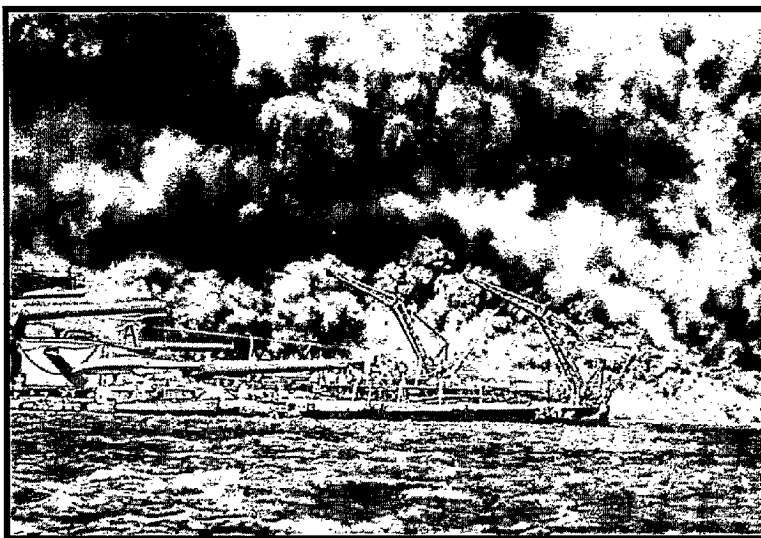


b7E





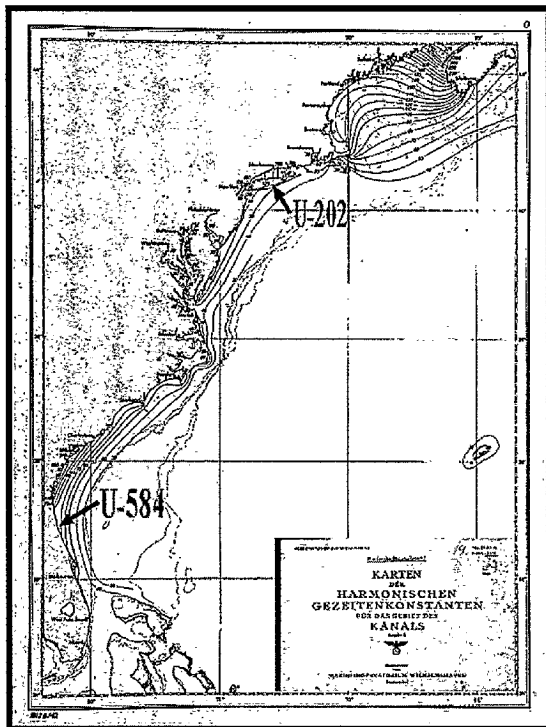
Pearl Harbor : December 7, 1941





World War II: 1942

Operation Pastorius





Operation Pastorius



German Saboteurs

New York Group



George John Dasch
Team Leader.
Advised FBI of the
operation. Imprisoned
and later deported to
Germany in 1948.



Ernest Peter Burger
Cooperated with
US authorities.
Imprisoned and later
deported to Germany
in 1948.



Richard Quirin
Executed on
August 8, 1942.



Heinrich Harn Heinck
Executed on
August 8, 1942.

German Saboteurs

Florida Group



Edward John Kerling
Team leader.
Executed on
August 8, 1942.



Hermann Otto Neubauer
Executed on
August 8, 1942.



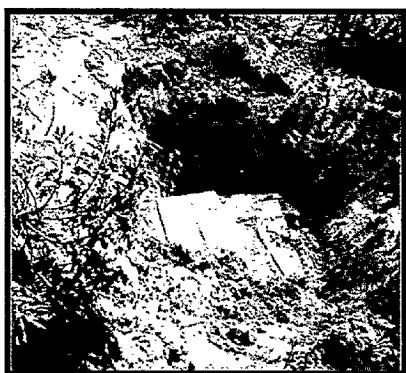
Herbert Hans Haupt
Executed on
August 8, 1942.



Werner Thiel
Executed on
August 8, 1942.



Operation Pastorius

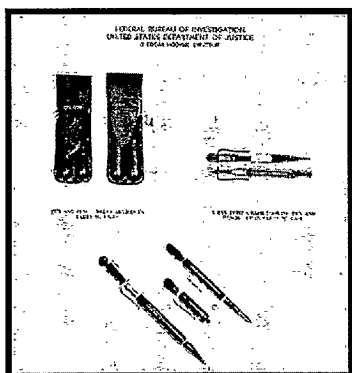
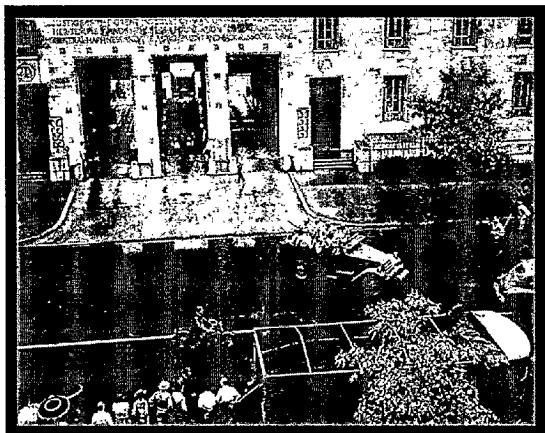


Seaman 2nd Class
John A. Cullen
USGC





Operation Pastorius





Operation Pastorius





Operation Tricycle



Dusko Popov





Operation Tricycle

• Hawaii – Ammunition dumps and mine depots

b7E



Operation Tricycle

• Aerodromes

b7E



Operation Tricycle

•Naval Strong Point Pearl Harbor

b7E



Government Rivals





US Intelligence Community (USIC) is Formed

National Security Act of 1947





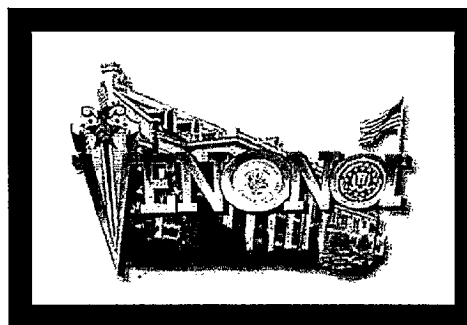


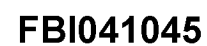
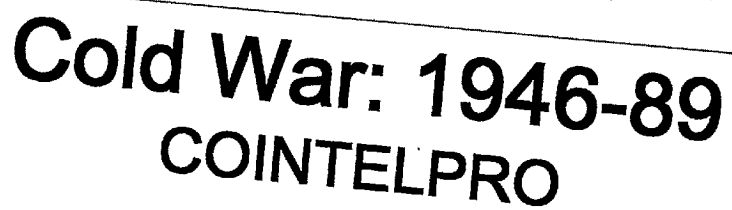
Cold War: 1946-89

Julius and Ethel Rosenberg Case



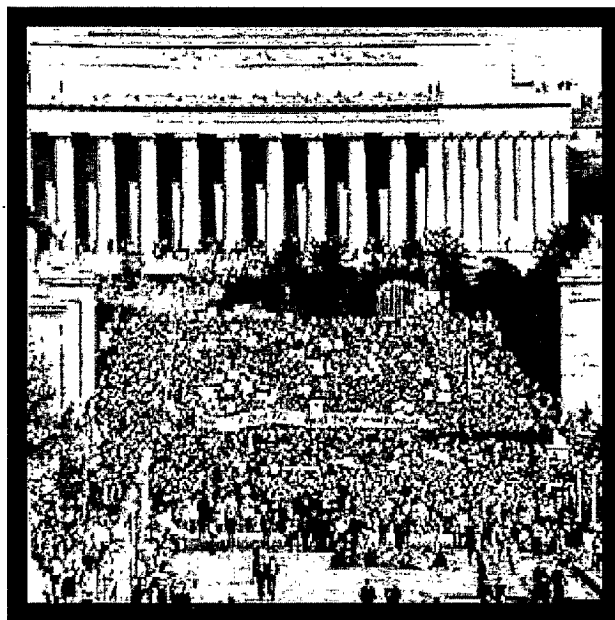
b7E







Vietnam War COINTELPRO





COINTELPRO

"We do not obtain authorization for "black bag" jobs from outside the Bureau. Such a technique involves trespassing and is clearly illegal; therefore, it would be impossible to obtain any legal sanction for it. Despite this, "black bag" jobs have been used because they represent an invaluable technique in combating subversive activities of a clandestine nature aimed directly at undermining and destroying our nation."

Memorandum. from W. C. Sullivan to C. D. DeLoach, 7/19/66, Subject: "Black Bag" Jobs



COINTELPRO

Congressional Investigations: 1970s

VI. WARRANTLESS FBI ELECTRONIC SURVEILLANCE OF AMERICAN CITIZENS

- May 20, 1969: Two members of the staff of the National Security Council
- May 29, 1969: A reporter for the "London Sunday Times"
- June 4, 1969: A reporter for the "New York Times"
- July 23, 1969: A White House domestic affairs adviser
- August 4, 1969: A White House speech writer
- September 10, 1969: A correspondent for CBS News
- May 4, 1970: A Deputy Assistant Secretary of State; a US Department of State official of Ambassador rank; and a Brigadier General with the US Department of Defense
- May 13, 1970: Two additional staff members of the National Security Council
- December 14, 1970: A second White House domestic affairs adviser

SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO
INTELLIGENCE ACTIVITIES
APRIL 23 (under authority of the order of April 14), 1976

Senator Frank Church
Idaho-D





COINTELPRO

- ◆ 65,000 domestic intelligence files opened
- ◆ 130,000 First Class letters opened/photographed
- ◆ 26,000 Americans placed on list to be taken into custody during a national emergency



New Guidelines and Orders

❖ Foreign Intelligence Surveillance Act (FISA)

❖ Attorney General Guidelines

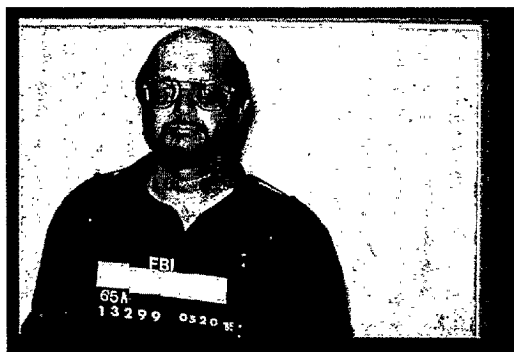


b7E



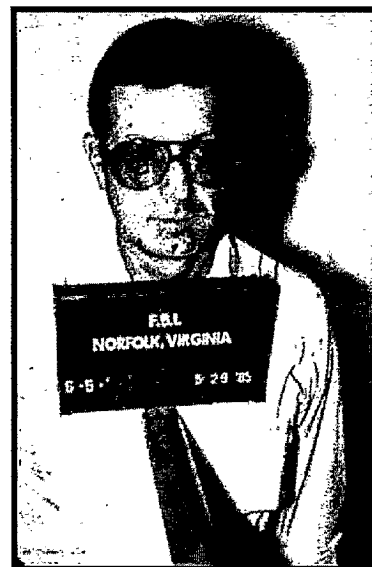
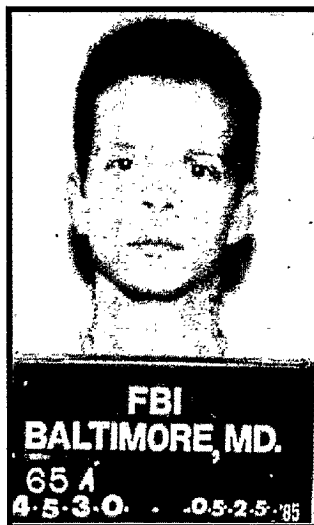
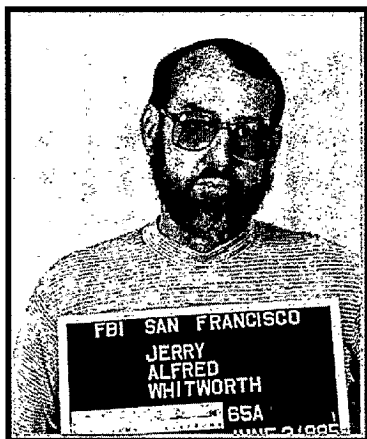
Cold War: 1946-89

Walker Espionage Ring





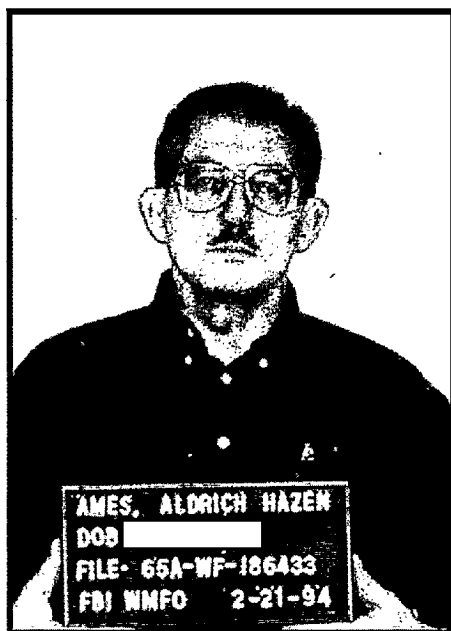
Walker Espionage Ring





Cold War/Post Cold War

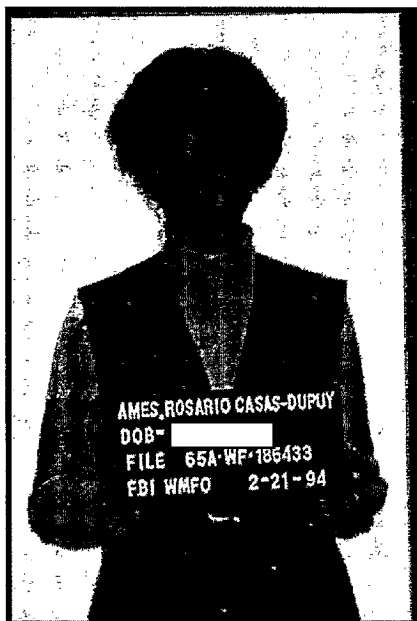
Aldrich H. Ames Espionage Case



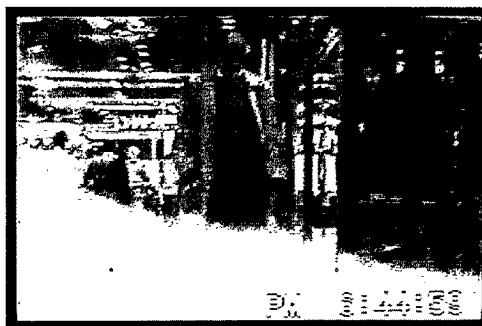
b6
b7c



Aldrich H. Ames Espionage Case



I AM READY TO MEET
AT B. ON 1 OCT.
I CANNOT READ
NORTH 13-19 SEPT.
IF YOU WILL
MEET AT B. ON 1 OCT.
PLS SIGNAL NORTH 4
OF 20 SEPT TO CONFIRM
NO MESSAGE AT PIPE.
IF YOU CANNOT MEET
1 OCT, SIGNAL NORTH AFTER
27 SEPT WITH MESSAGE AT
PIPE.



b6
b7C



Cold War/Post Cold War

Robert P. Hanssen Espionage Case



b6
b7C



Post Cold War

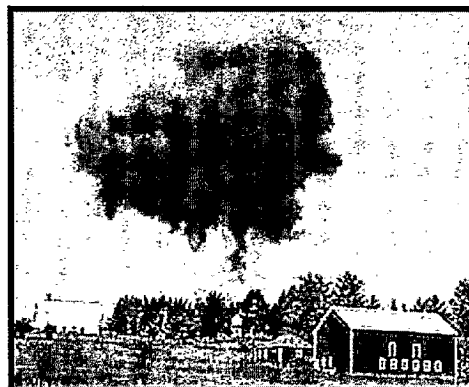
Brian P. Regan Espionage Case



b6
b7c



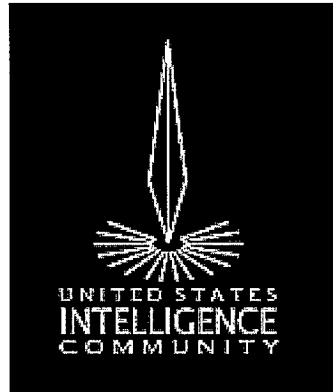
9-11





Counterintelligence Today

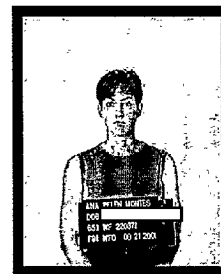
USIC



Intelligence Reform and Terrorism Prevention Act of 2004



Summary



b6
b7c

6	N	n	b	h	1	X
3	v	l	u	8	4	w
1	e	m	3	f	5	g
5	t	a	9	0	i	d
2	k	7	2	8	6	s
4	p	o	y	c	f	g
1 3 6 2 5 4						

	4	3	6	7	Ø	1	8
	A	T	I	L	N	E	S
2	B	C	D	F	G	H	J
5	K	M	Ñ	O	P	Q	R
9	U	V	W	X	Y	Z	

011011007 FN Q13
FBI
LABORATORY

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 12-22-2011 BY 65179 DMH/STW



FBI Counterintelligence Support to the US Department of Defense

~~SECRET//NOFORN~~

Counterintelligence Strategic Goals

- Prevent proliferation of chemical, biological, radiological, nuclear and high-yield explosive information, technology, and materials
- Prevent the penetration of the United States Intelligence Community
- Prevent the penetration of other government agencies and their contractors
- Prevent the compromise of Critical National Assets



~~SECRET//NOFORN~~

Program Objectives and Outcomes

- Identify intelligence service objectives, officers, assets, and operations
- Disrupt the operations of intelligence services
- Change the behavior of exploited institutions and individuals

~~SECRET//NOFORN~~

Program Strategies

- Know the domain
- Engage in strategic partnerships
- Conduct sophisticated CI operations
- Understand the threat
- Inform policymakers

~~SECRET//NOFORN~~

Strategic Partnerships

- CI Working groups in each field office, including field agents and intelligence analysts.
- Working groups routinely share relevant strategic and tactical information with federal, state and local law enforcement and government agencies
- National CI Working Group – Led by the FBI and comprising 25 representatives from other intelligence agencies. The goal is to better coordinate CI operations throughout the Intelligence Community
- Regional Counterintelligence Working Groups from a broad spectrum of intelligence agencies work together around the country to identify policy issues and coordinate operations

~~SECRET//NOFORN~~

Coverage Across America



FBI
FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE
One full-time agent per 100,000 population. The FBI is the largest law enforcement agency in the United States.

~~SECRET//NOFORN~~

7/14/2011

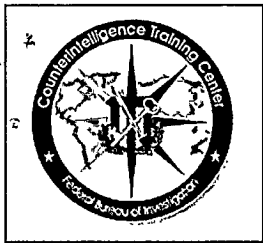
Questions?

-
- FBIHQ
-



~~SECRET//NOFORN~~

b6
b7C



~~SECRET~~

~~SECRET/NOFORN~~

Name: _____
Date: _____

Counterintelligence Investigations and Operations

PRETEST

[Redacted]

[Redacted]

DATE: 11-04-2011
CLASSIFIED BY 65179 DMH/STW
REASON: 1.4 (C)
DECLASSIFY ON: 11-04-2036

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

[Redacted]

b7E

~~SECRET~~

~~SECRET/NOFORN~~

FBI041063

copy



~~SECRET~~

~~SECRET/NOFORN~~

Name: _____

Date: _____

Counterintelligence Investigations and Operations

PRETEST

Correct answers are in RED

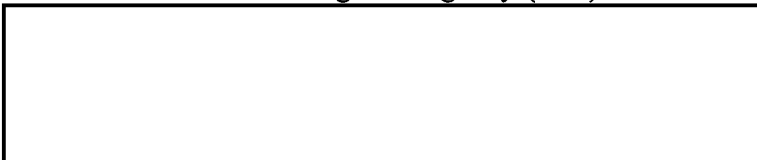
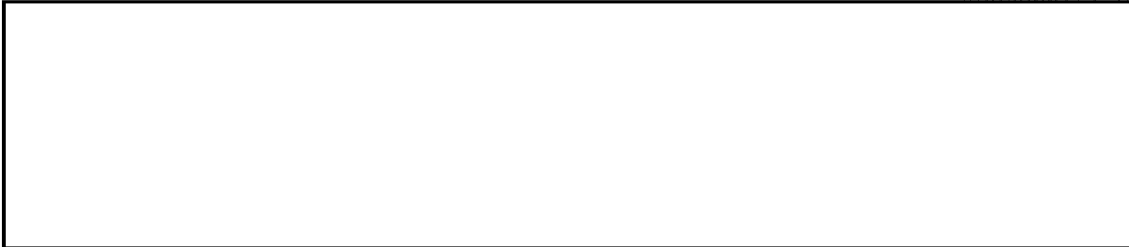
Requests for help or information are in blue.

DATE: 11-04-2011

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

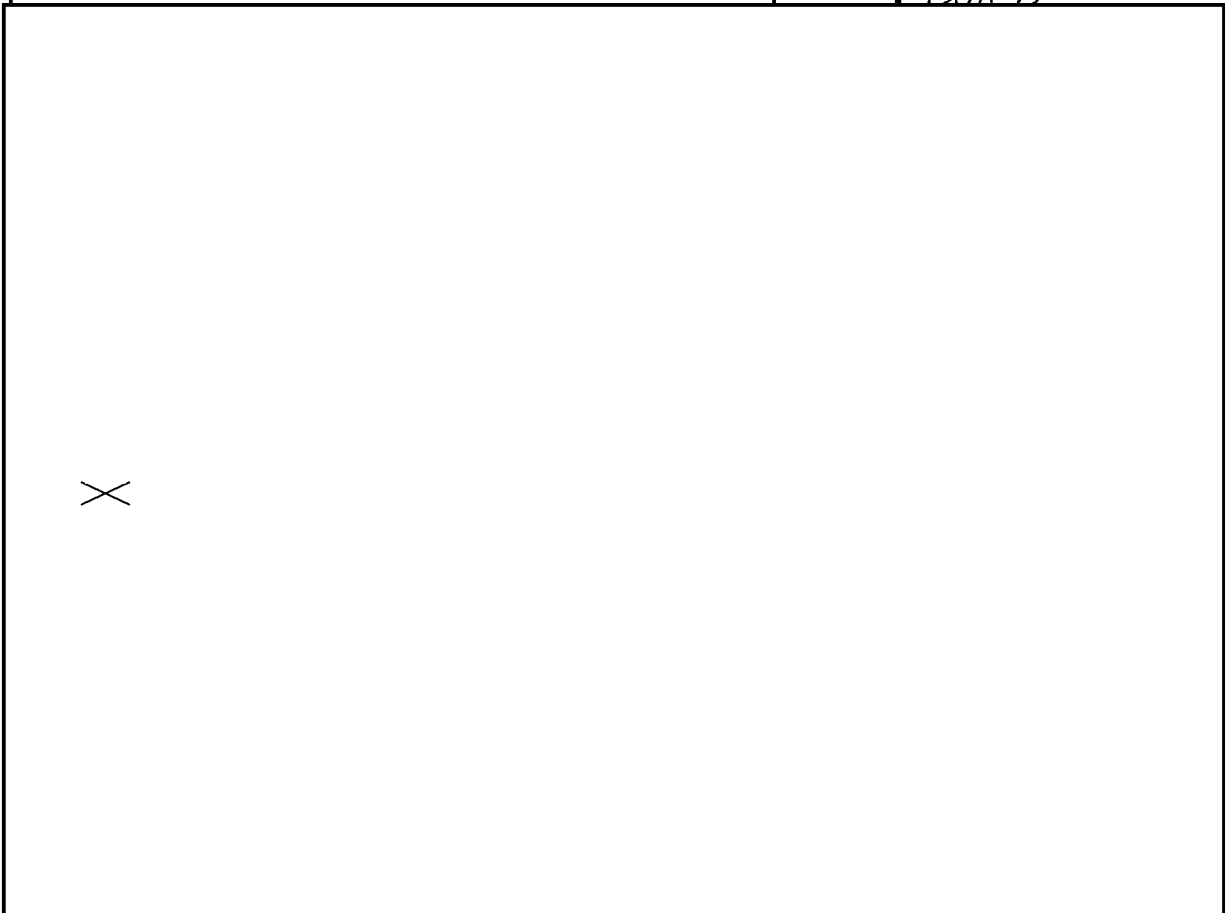
DECLASSIFY ON: 11-04-2036



ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

1 copy

b7E



~~SECRET~~

~~SECRET/NOFORN~~

FBI041064



CI Strategic [redacted] Targeting Course 10-01
November 17-19, 2009
[redacted]

b6
b7C
b7E

Monday, 11/16	Tuesday, 11/17	Wednesday, 11/18	Thursday, 11/19	Friday, 11/20
TRAVEL DAY	8:00 am – 8:30 am Welcome / Admin Matters SSA [redacted] CITC Staff 8:30 am – 9:00 am A/ASC [redacted] Course Overview / Intro / Questions 9:00 am – 9:15 am Break 9:15 am – 11:00 am SA [redacted] “The Long Tail of Counterintelligence” 11:00 am – 1:00 pm LUNCH 1:00 pm – 4:00 pm [redacted] “Best Practices” and CI Task Force Panel”	8:30 am – 9:30 am [redacted] UCE Ops SSA [redacted] 9:30 am – 9:45 am Break 9:45 am – 10:45 am Interacting With the Academic Community [redacted] 10:45 am - 11:00 am Break 11:00 am – 12:00 am Tech Transfer Case Presentation SA [redacted] 12:00 pm – 1:00 pm LUNCH 1:00 pm – 1:45 pm “Theft of Trade Secrets” Case Presentation SA [redacted] 1:45 pm – 2:00 pm Break 2:00 pm – 2:45 pm CI Cyber Presentation SSA [redacted] 3:00 pm – 4:30 pm [redacted] Scientists and Professors Guest Speaker	8:30 am – 12:00 pm [redacted] Human Source Recruiting SSA [redacted] 12:00 pm – 1:00 pm LUNCH 1:00 pm – 4:00 pm [redacted] Human Source Recruiting (cont) SSA [redacted] Course wrap up and critiques	TRAVEL DAY

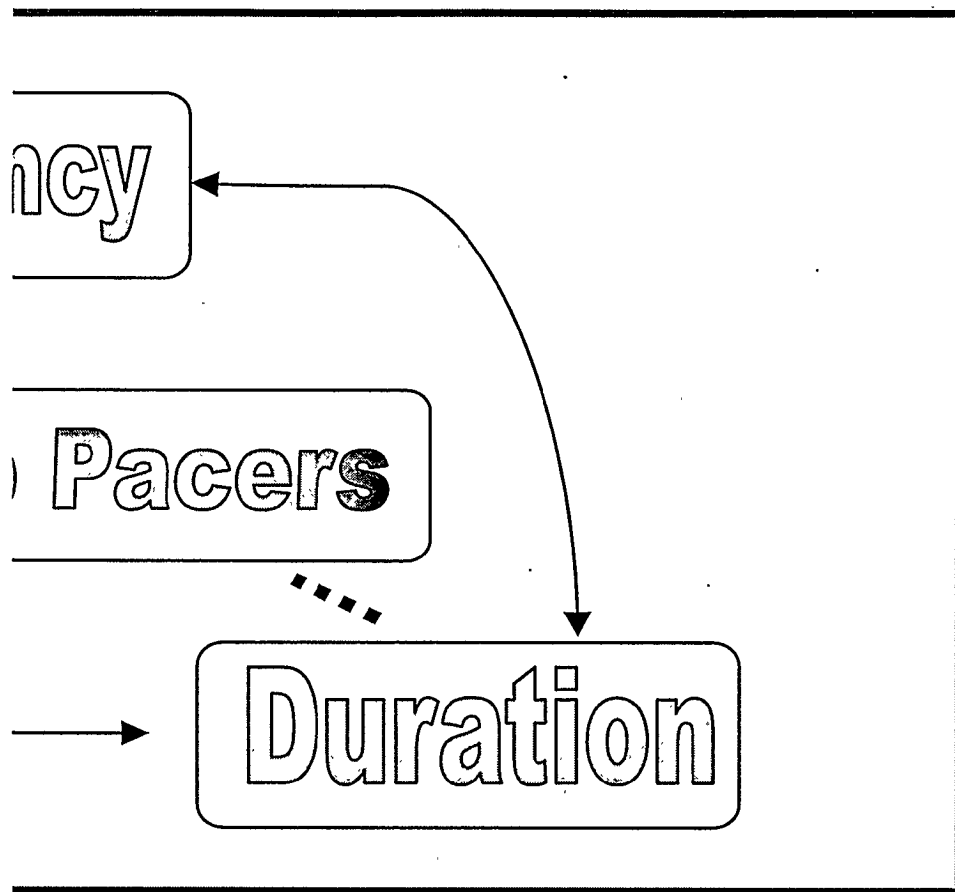


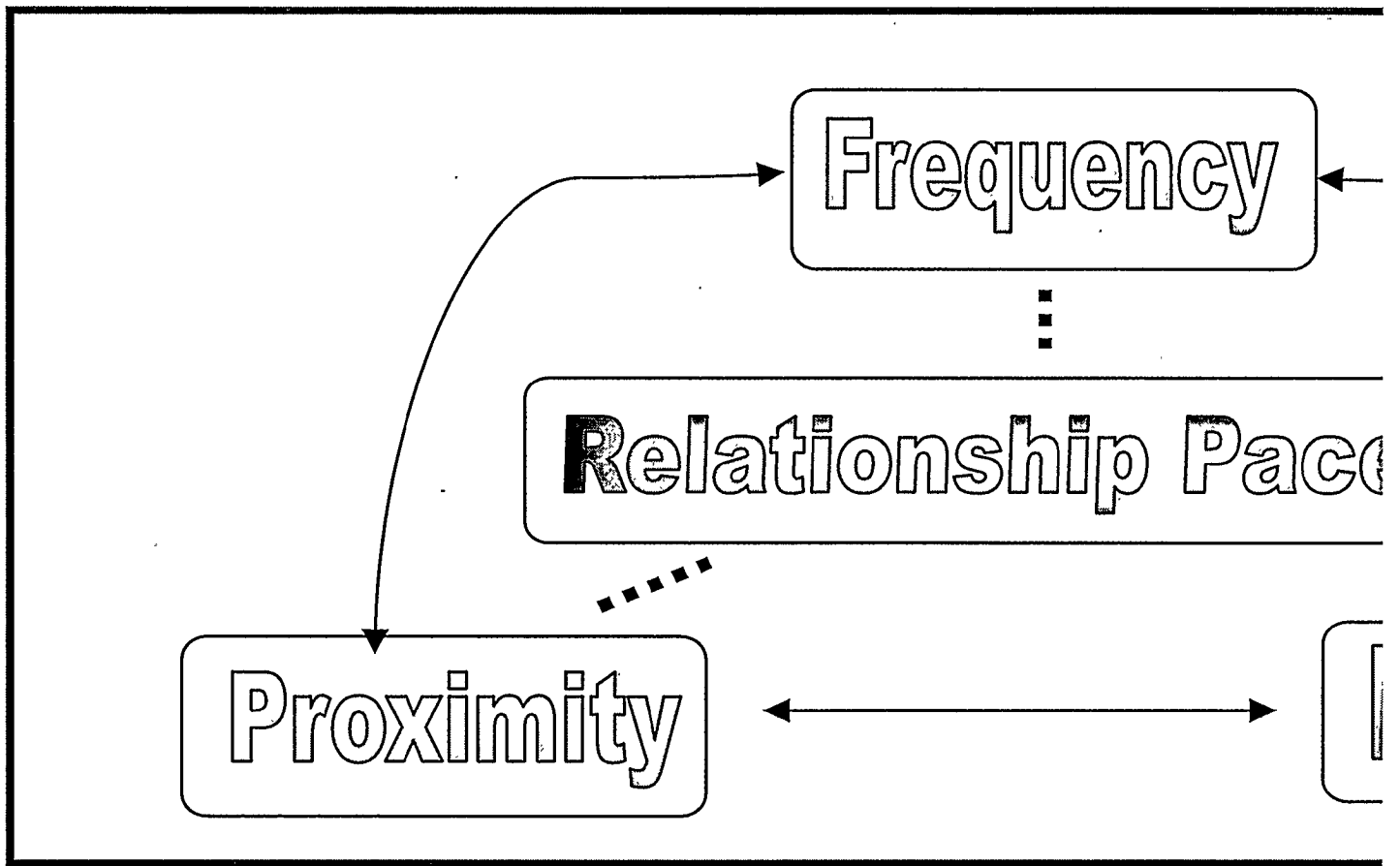
CI Strategic Targeting Course

b7E

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-18-2012 BY 65179 DMH/STW









Counterintelligence Strategic [Redacted] Targeting Course Overall Evaluation

11/17/2008 – 11/21/2008

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-18-2012 BY 65179 DMH/STW

b7E

Instructions: Please circle yes or no after each statement. If you select no, please provide a brief reason as why you feel that way. Regarding the specific blocks of instruction, please provide comments and/or suggestions that will help us to better meet your needs and interests.

- | | | |
|--|-----|----|
| 1. The material covered during the course was relevant to my job. | Yes | No |
| 2. The material I learned will be useful in the performance of my duties. | Yes | No |
| 3. The audio/visual aids and handouts (if applicable) were effective. | Yes | No |
| 4. A discussion of the course objectives enabled me to set appropriate expectations for the class. | Yes | No |
| 5. The material was presented in an interesting manner. | Yes | No |
| 6. The instructors were effective communicators. | Yes | No |

Comments:

Domain Operations Course

Day 2

Guest Speaker	8:00am-8:50am
Adult Learning	9:00am-10:30am
Psychology of AL	9:00am-9:30am
Motivation of AL	9:30am-10:00am
Know Your Audience	10:00am-10:30am
Instructional Design	10:30am-1:50pm
Goals & Objectives	10:30am-11:30am
Role of Presenter	11:30am-12:00pm
Methods of Instruction	1:00pm-1:50pm
Dynamic Presentations	2:00pm-2:50pm
Impromptu Presentations	3:00pm-5:00pm

Thursday	Day 3	Block Name	Instructor	
		Group Breakout and Presentation Prep: 15 - 30 minutes explaining what to do. Class will break into their 4 groups and work together on strengthening their individual presentations. Each individual will make a 15 minute presentation the next day to the entire group with praise and polish to follow.		b6 b7C
8:00 AM	10:00 AM	2.00		
10:00 AM	10:50 AM	1.00	Group 1 presentations: Followed with Praise and Polish	Attendees
11:00 AM	12:00 PM	1.00	Group 2 Presentations: Followed with Praise and Polish	Attendees
12:00 PM	1:00 PM	1.00	Lunch	
1:00 PM	2:00 PM	1.00	Group 3 Presentations: Followed with Praise and Polish	Attendees
2:00 PM	3:00 PM	1.00	Group 4 Presentations: Followed with praise and polish	Attendees
3:10 PM	3:30 PM	0.50	Guided discussion on best practices / lessons learned from the presentations	SSA [redacted] / CITC
3:40 PM	5:00 PM	1.50	[redacted] / Best Practices guest speaker	[redacted]
		0.50	Course wrap up and critiques	SSA [redacted]
Friday	Day 4	Block Name	Instructor	
		TRAVEL DAY	SSA [redacted]	b6 b7C

[redacted] will provide speaker and / or best practices presentation

Wednesday Day 2		Block Name	Instructor	
		Business Alliance Guest Speaker: (The hosting field office will provide a Business Alliance Speaker from their own domain. The talking topics should include perceptions of the FBI and best practices for presentations and relationship development.)		
8:00 AM	8:50 AM	1.00		
8:00 AM	10:30 AM	2.50		
		0.50		
		0.50		
		0.50		
10:30 AM	1:50 AM	3.50		
		1.00		
		0.50		
		1.00		
2:00 PM	2:50 PM	1.00		
3:00 PM	5:00 PM	2.00		

b6
b7C

Counterintelligence Domain Operations Course

Version 1.01

Tuesday	Day 1	Time	Block Name	Instructor	Logistics and Admin	Scheduling Notes
7:30 AM	8:00 AM	0.50	Admin / Introductions / Course Orientation: [redacted] will do this)	SSA [redacted]	Handout: PLATINUM RULE	b6 b7C b7E
8:00 AM	8:50 AM	1.00	FBI, Perceptions vs. Reality:	[redacted]		
9:00 AM	9:50 AM	1.00	The [redacted] Threat / Domain Strategy [redacted]	[redacted]	Attempt to have [redacted] do this block	
10:00 AM	11:20 AM	1.00	Academic Guest Speaker:	[redacted]	This speaker will be provided from the hosting field office and be from the academic alliance background.	
11:30 AM	12:20 PM	1.00	LUNCH			
12:30 PM	3:00 PM	2.50	Behavioral Relationship Building	[redacted]		b6 b7C
3:00 PM	5:00 PM	2.00	Specialized Interview Strategies for CEO's and ranking academics:	[redacted]		

~~Secret/Noform~~

DATE: 01-13-2012

CLASSIFIED BY 65179 DMH/STW

REASON: 1.4 (C)

DECLASSIFY ON: 01-13-2037

~~SECRET~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

~~SECRET/NOFORM~~



Regional Counterintelligence Work Group [Redacted] Threat

SSA [Redacted] March 1, 2007
FBI WFO
Domain Task Force

~~Secret/Noform~~

~~SECRET/NOFORM~~



[Redacted] Threat

- I. Definition of [Redacted] Threat
- II. Strategies to stem the [Redacted] Threat
- III. Success Stories
- IV. Strengthening the Regional Approach to this threat

~~Secret/Noform~~

b6
b7C
b7E

~~SECRET/NOFORM~~



Evolution of CI Efforts

Cold War focus on [Redacted] threat

(S) [Redacted]

- Diplomatic embassies, UN Missions, Consulates

Major Changes in the CI threat posture

- Fall of the Berlin Wall, end of the Cold War
- Globalization of communications, commerce

~~Secret/Noform~~

~~SECRET/NOFORM~~



Defining the [Redacted] Threat

(S) [Redacted]

~~Secret/Noform~~

b1
b7E

~~SECRET/NOFORM~~



Defining the [Redacted] Threat

Entities from a record number of countries - 108 -- were involved in collection against US interests.

(S) [Redacted]

~~Secret/Noform~~

~~SECRET/NOFORM~~



CI [Redacted] Strategy

(S) [Redacted]

- Eroded US military advantage by shortening development cycle of sophisticated technology
- Undercut US economy by enabling foreign firms to gain a competitive economic advantage over US companies

~~Secret/Noform~~

b1
b7E

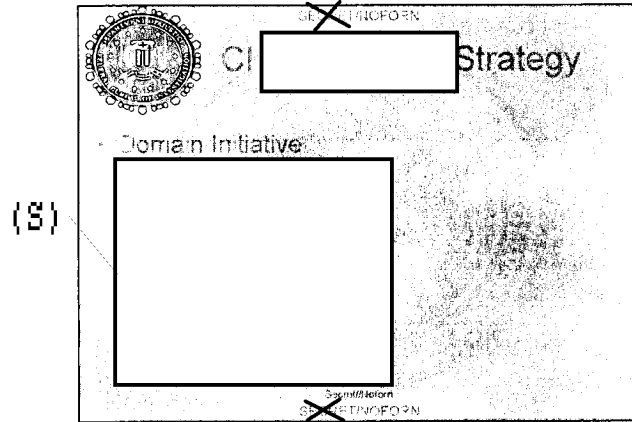
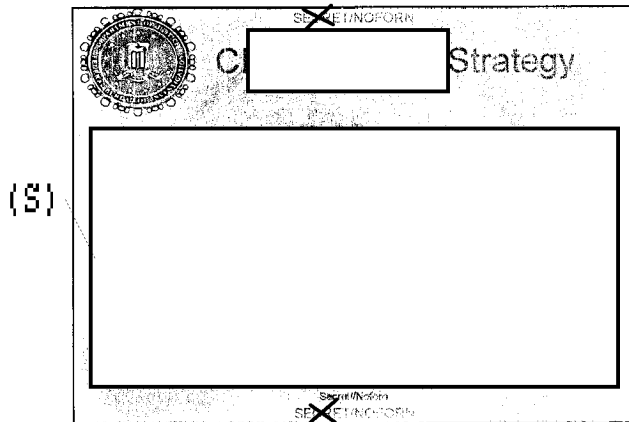
~~Secret/Noform~~

ACLURM042174

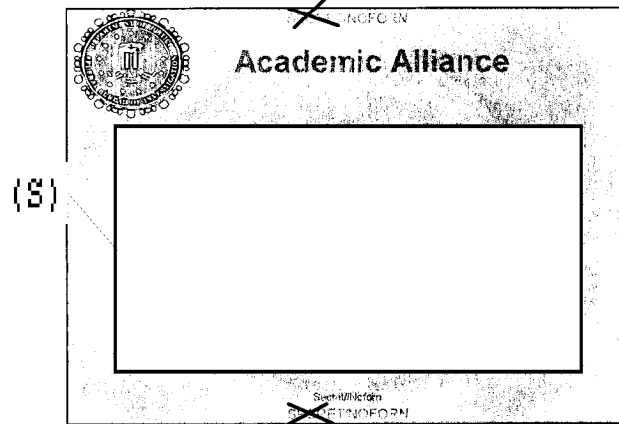
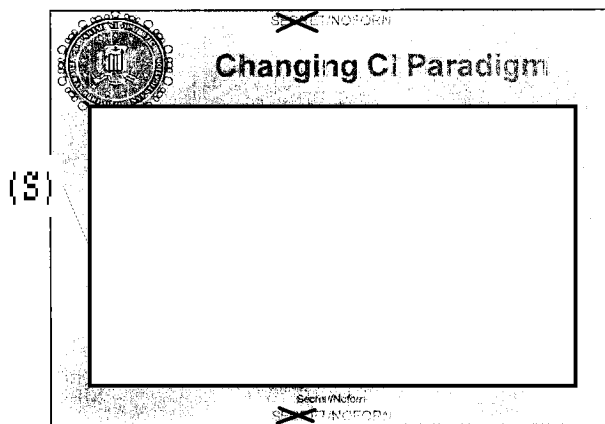
FBI041074

~~Secret/Noform~~

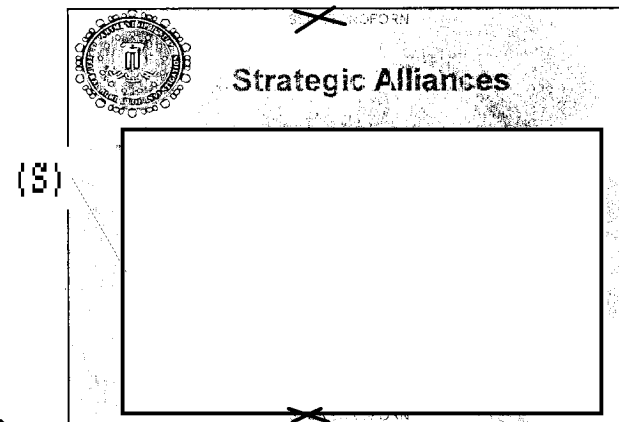
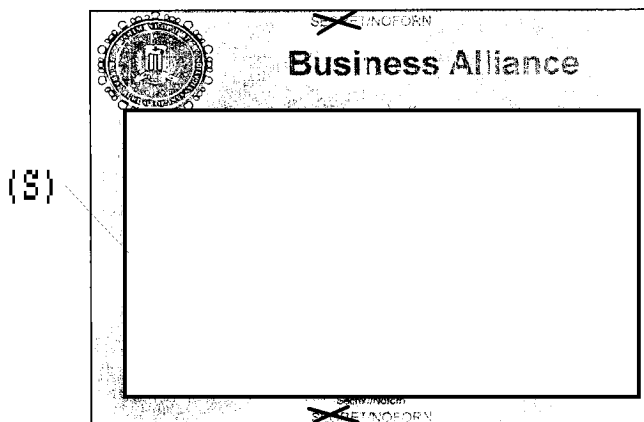
~~SECRET~~



b1
b7E



b1
b7E



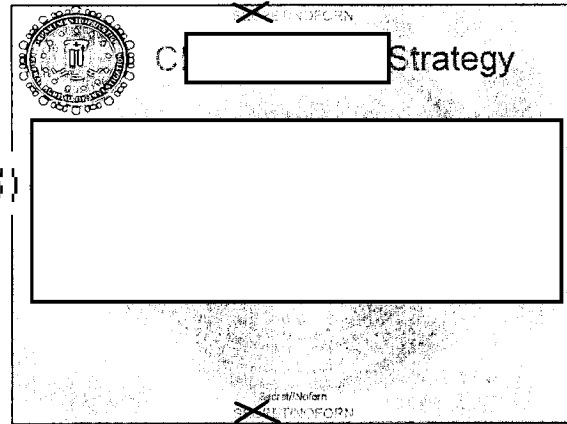
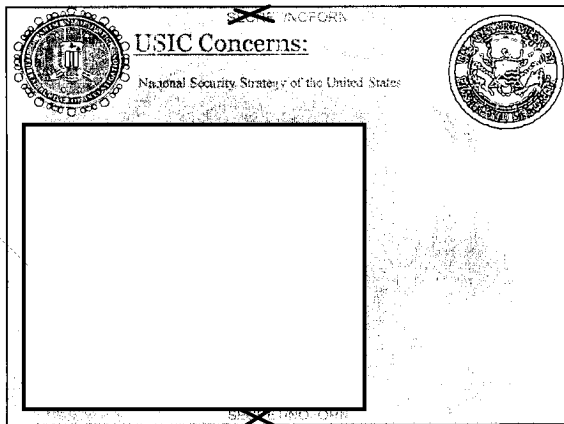
b1
b7E

~~SECRET~~

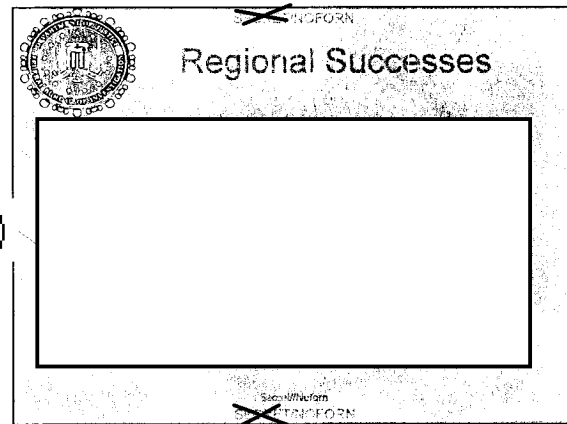
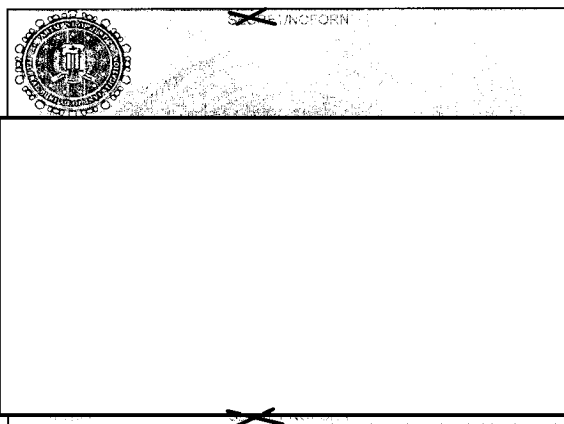
~~Secret/Noform~~

~~Secret/Noform~~

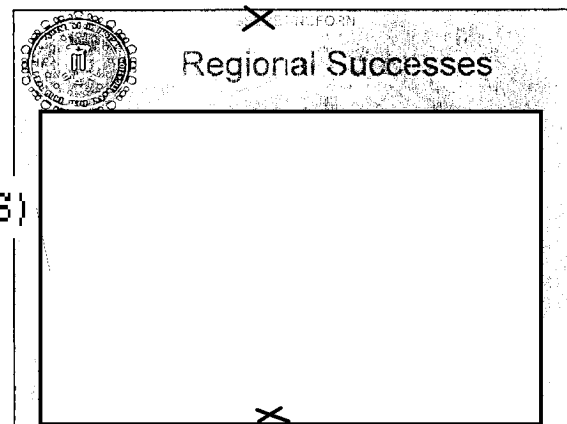
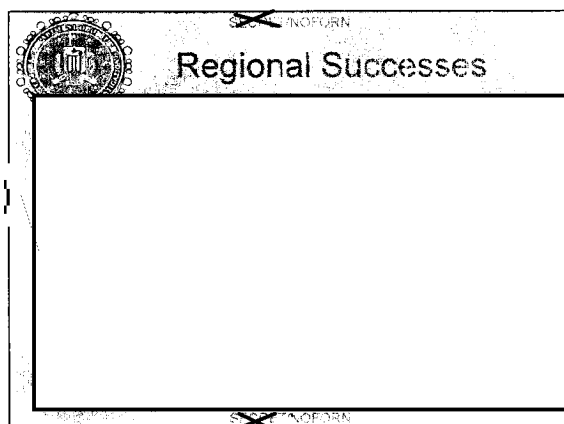
~~SECRET~~



b1
b7E



b1
b7E



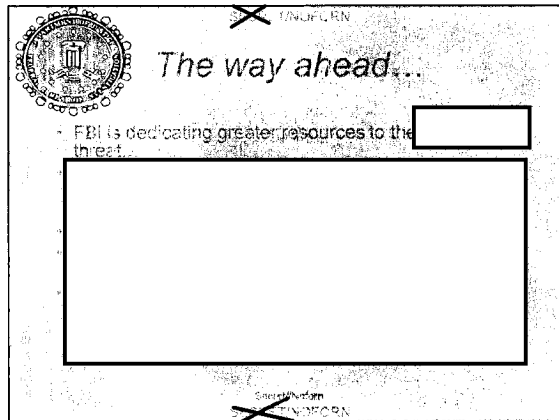
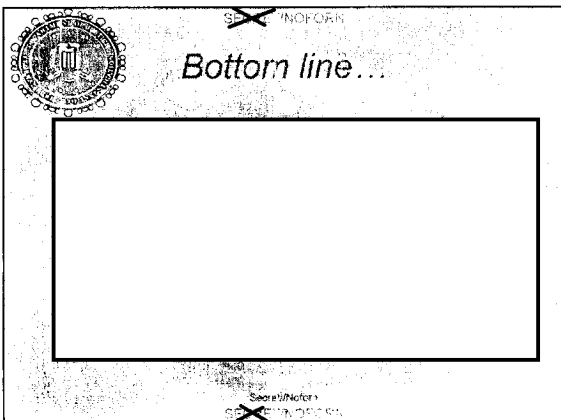
b1
b7E

~~Secret/Noform~~

~~SECRET~~

~~Secret/Noform~~

~~SECRET~~



b7E

~~SECRET~~

~~Secret/Noform~~

Discovery Request

Counterintelligence Strategic

Targeting Course

b7E

2008-Mark 17, 2010

Course introduced in 2008

Ready to go!
vm

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-17-2012 BY 65179 DMH/STW

THE PLATINUM RULE

DISCOVER THE FOUR BASIC
BUSINESS PERSONALITIES—
AND HOW THEY CAN
LEAD YOU TO SUCCESS

“Full of take-action strategies. A learning
and earning tool for the times. Don’t underestimate
the power of this fine book.”—Harvey Mackay,
author of *Swim with the Sharks Without Being Eaten Alive*

Tony Alessandra, Ph.D., and
Michael J. O’Connor, Ph.D.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ Unrecorded Serial

Delete Page(s) ~ 181
b7E
b7F
b7G
b7H
b7I
b7J
b7K
b7L
b7M
b7N
b7O
b7P
b7Q
b7R
b7S
b7T
b7U
b7V
b7W
b7X
b7Y
b7Z
b7AA
b7AB
b7AC
b7AD
b7AE
b7AF
b7AG
b7AH
b7AI
b7AJ
b7AK
b7AL
b7AM
b7AN
b7AO
b7AP
b7AQ
b7AR
b7AS
b7AT
b7AU
b7AV
b7AW
b7AX
b7AY
b7AZ
b7BA
b7BB
b7BC
b7BD
b7BE
b7BF
b7BG
b7BH
b7BI
b7BJ
b7BK
b7BL
b7BM
b7BN
b7BO
b7BP
b7BQ
b7BR
b7BS
b7BT
b7BU
b7BV
b7BW
b7BX
b7BY
b7BZ
b7CA
b7CB
b7CC
b7CD
b7CE
b7CF
b7CG
b7CH
b7CI
b7CJ
b7CK
b7CL
b7CM
b7CN
b7CO
b7CP
b7CQ
b7CR
b7CS
b7CT
b7CU
b7CV
b7CW
b7CX
b7CY
b7CZ
b7DA
b7DB
b7DC
b7DD
b7DE
b7DF
b7DG
b7DH
b7DI
b7DJ
b7DK
b7DL
b7DM
b7DN
b7DO
b7DP
b7DQ
b7DR
b7DS
b7DT
b7DU
b7DV
b7DW
b7DX
b7DY
b7DZ
b7EA
b7EB
b7EC
b7ED
b7EE
b7EF
b7EG
b7EH
b7EI
b7EJ
b7EK
b7EL
b7EM
b7EN
b7EO
b7EP
b7EQ
b7ER
b7ES
b7ET
b7EU
b7EV
b7EW
b7EX
b7EY
b7EZ
b7FA
b7FB
b7FC
b7FD
b7FE
b7FF
b7GG
b7GH
b7GI
b7GJ
b7GK
b7GL
b7GM
b7GN
b7GO
b7GP
b7GQ
b7GR
b7GS
b7GT
b7GU
b7GV
b7GW
b7GX
b7GY
b7GZ
b7HA
b7HB
b7HC
b7HD
b7HE
b7HF
b7HG
b7HH
b7HI
b7HJ
b7HK
b7HL
b7HM
b7HN
b7HO
b7HP
b7HQ
b7HR
b7HS
b7HT
b7HU
b7HV
b7HW
b7HX
b7HY
b7HZ
b7IA
b7IB
b7IC
b7ID
b7IE
b7IF
b7IG
b7IH
b7II
b7IJ
b7IK
b7IL
b7IM
b7IN
b7IO
b7IP
b7IQ
b7IR
b7IS
b7IT
b7IU
b7IV
b7IW
b7IX
b7IY
b7IZ
b7JA
b7JB
b7JC
b7JD
b7JE
b7JF
b7JG
b7JH
b7JI
b7JJ
b7JK
b7JL
b7JM
b7JN
b7JO
b7JP
b7JQ
b7JR
b7JS
b7JT
b7JU
b7JV
b7JW
b7JX
b7JY
b7JZ
b7KA
b7KB
b7KC
b7KD
b7KE
b7KF
b7KG
b7KH
b7KI
b7KJ
b7KK
b7KL
b7KM
b7KN
b7KO
b7KP
b7KQ
b7KR
b7KS
b7KT
b7KU
b7KV
b7KW
b7KX
b7KY
b7KZ
b7LA
b7LB
b7LC
b7LD
b7LE
b7LF
b7LG
b7LH
b7LI
b7LJ
b7LK
b7LL
b7LM
b7LN
b7LO
b7LP
b7LQ
b7LR
b7LS
b7LT
b7LU
b7LV
b7LW
b7LX
b7LY
b7LZ
b7MA
b7MB
b7MC
b7MD
b7ME
b7MF
b7MG
b7MH
b7MI
b7MJ
b7MK
b7ML
b7MM
b7MN
b7MO
b7MP
b7MQ
b7MR
b7MS
b7MT
b7MU
b7MV
b7MW
b7MX
b7MY
b7MZ
b7NA
b7NB
b7NC
b7ND
b7NE
b7NF
b7NG
b7NH
b7NI
b7NJ
b7NK
b7NL
b7NM
b7NN
b7NO
b7NP
b7NQ
b7NR
b7NS
b7NT
b7NU
b7NV
b7NW
b7NX
b7NY
b7NZ
b7OA
b7OB
b7OC
b7OD
b7OE
b7OF
b7OG
b7OH
b7OI
b7OJ
b7OK
b7OL
b7OM
b7ON
b7OO
b7OP
b7OQ
b7OR
b7OS
b7OT
b7OU
b7OV
b7OW
b7OX
b7OY
b7OZ
b7PA
b7PB
b7PC
b7PD
b7PE
b7PF
b7PG
b7PH
b7PI
b7PJ
b7PK
b7PL
b7PM
b7PN
b7PO
b7PP
b7PQ
b7PR
b7PS
b7PT
b7PU
b7PV
b7PW
b7PX
b7PY
b7PZ
b7QA
b7QB
b7QC
b7QD
b7QE
b7QF
b7QG
b7QH
b7QI
b7QJ
b7QK
b7QL
b7QM
b7QN
b7QO
b7QP
b7QQ
b7QR
b7QS
b7QT
b7QU
b7QV
b7QW
b7QX
b7QY
b7QZ
b7RA
b7RB
b7RC
b7RD
b7RE
b7RF
b7RG
b7RH
b7RI
b7RJ
b7RK
b7RL
b7RM
b7RN
b7RO
b7RP
b7RQ
b7RR
b7RS
b7RT
b7RU
b7RV
b7RW
b7RX
b7RY
b7RZ
b7SA
b7SB
b7SC
b7SD
b7SE
b7SF
b7SG
b7SH
b7SI
b7SJ
b7SK
b7SL
b7SM
b7SN
b7SO
b7SP
b7SQ
b7SR
b7SS
b7ST
b7SU
b7SV
b7SW
b7SX
b7SY
b7SZ
b7TA
b7TB
b7TC
b7TD
b7TE
b7TF
b7TG
b7TH
b7TI
b7TJ
b7TK
b7TL
b7TM
b7TN
b7TO
b7TP
b7TQ
b7TR
b7TS
b7TT
b7TU
b7TV
b7TW
b7TX
b7TY
b7TZ
b7UA
b7UB
b7UC
b7UD
b7UE
b7UF
b7UG
b7UH
b7UI
b7UJ
b7UK
b7UL
b7UM
b7UN
b7UO
b7UP
b7UQ
b7UR
b7US
b7UT
b7UU
b7UV
b7UW
b7UX
b7UY
b7UZ
b7VA
b7VB
b7VC
b7VD
b7VE
b7VF
b7VG
b7VH
b7VI
b7VJ
b7VK
b7VL
b7VM
b7VN
b7VO
b7VP
b7VQ
b7VR
b7VS
b7VT
b7VU
b7VV
b7VW
b7VX
b7VY
b7VZ
b7WA
b7WB
b7WC
b7WD
b7WE
b7WF
b7WG
b7WH
b7WI
b7WJ
b7WK
b7WL
b7WM
b7WN
b7WO
b7WP
b7WQ
b7WR
b7WS
b7WT
b7WU
b7WV
b7WW
b7WX
b7WY
b7WZ
b7XA
b7XB
b7XC
b7XD
b7XE
b7XF
b7XG
b7XH
b7XI
b7XJ
b7XK
b7XL
b7XM
b7XN
b7XO
b7XP
b7XQ
b7XR
b7XS
b7XT
b7XU
b7XV
b7XW
b7XX
b7XY
b7XZ
b7YA
b7YB
b7YC
b7YD
b7YE
b7YF
b7YG
b7YH
b7YI
b7YJ
b7YK
b7YL
b7YM
b7YN
b7YO
b7YP
b7YQ
b7YR
b7YS
b7YT
b7YU
b7YV
b7YW
b7YX
b7YY
b7YZ
b7ZA
b7ZB
b7ZC
b7ZD
b7ZE
b7ZF
b7ZG
b7ZH
b7ZI
b7ZJ
b7ZK
b7ZL
b7ZM
b7ZN
b7ZO
b7ZP
b7ZQ
b7ZR
b7ZS
b7ZT
b7ZU
b7ZV
b7ZW
b7ZX
b7ZY
b7ZZ

b7C
 b7C
 b7C
 b7E
 b7E
 b7E

b7C, b7E
b7C, b7E
b7C, b7E

b7E
b7E
b7E

[illegible]

No Duplet Page
FBI041082

[illegible]

No Duplicate Pages
FBI041083

No Duplicate Pages
FBI041084