
NATIONAL COUNTERINTELLIGENCE CENTER
UNITED STATES OF AMERICA

CHAPTER 4

CHAPTER 4

Counterintelligence at the End Of the 20th Century

Introduction

The breakup of the Soviet Union in 1991 and its ongoing volatile political environment, the liberation of Eastern Europe, and the reunification of Germany all led people in the United States to believe that espionage was out-of-date and the foreign intelligence war over. But the beginning of the post-Cold War did not signal the end of espionage.

In 1994 the nation was hit by a bombshell when the FBI arrested Hazen Aldrich Ames, a senior CIA officer, for spying for almost 10 years for the Russians. The deadly consequences of Ames' personal betrayal and the compromise of national security drastically altered US counterintelligence. Congress was furious about this "failure" and demanded change. To preclude any action by Congress to legislate changes in counterintelligence, President Clinton issued Presidential Decision Directive/NSC-24 on 3 May 1994, which reorganized counterintelligence.

Under the Executive Order, a National Counterintelligence Policy Board (NACIPB) was created to coordinate CI activities and resolve interagency disagreements. The NACIPB, unlike previous groups, reports to the National Security Council. In addition, the order created a National Counterintelligence Center (NACIC) to share and evaluate information regarding foreign intelligence threats.

In 1995, Congress recognized that countries that formerly had not been considered intelligence threats were stealing American technology and decided to take action. They enacted legislation, the Economic Espionage Act of 1996, which the President signed on 11 October 1996. In April 1997, the first conviction under the new law took place with the sentencing in Pennsylvania of Daniel Worthing.

The nation again was reminded in 1996 that traditional espionage did not take a holiday when Robert Chaegon Kim, a computer specialist in the Maritime Systems Directorate of the Office of Naval Intelligence, was arrested on 25 September 1996 on charges of passing classified information to South Korea. Almost two months later, Harold J. Nicholson, a 16-year CIA veteran and former station chief with access to "very damaging information," was arrested on 15 November 1996 and charged with passing Top Secret information to the Russians. A month later, on 17 December 1996, Earl E. Pitts, a Special Agent with the FBI since 1983, was arrested and charged with compromising FBI intelligence operations to the SVRR, successor to the Soviet KGB.

This chapter is not complete. There are two more years before the beginning of the 21st Century and, during this time, additional spies will undoubtedly be detected, arrested, or neutralized. Threats to our nation's national security will continue unabated as the rest of the world looks at the United States as the "great Satan," the technology store to be robbed, the "bullying big brother," or a target to knock down to size. New technological advances in communications and information sharing will also create new difficulties for American counterintelligence to resolve. All of these developments indicate that US counterintelligence will continue to face threats to the national security in the future.

The Jacobs Panel

On 23 May 1990, a blue-ribbon panel, called the Jacobs panel after its chairman Eli Jacobs, reported its recommendations to the Senate Intelligence Committee. The panel had been asked by the chairmen of the Committee, Senator David L. Boren, Democrat of Oklahoma and Senator William S. Cohen, Republican of Maine, to review espionage cases from the 1980s and to make recommendations to change the nation's espionage laws.

The eight-member panel suggested 13 legislative proposals. According to Jacobs, "The past 20 years of espionage indicate that the main threat is not the ideologically motivated spy but rather the voluntary spy-the insider who betrays his country not from belief, but for money or revenge."

The Senate Committee was told that the panel looked at 19 espionage cases from 1975 to the present day and found that most of the people studied had access to Top Secret or codeword information. They also visited the CIA, FBI, Pentagon, National Security Agency, and others. Both the CIA and FBI said they offered suggestions but did not identify them.

In making its recommendations, the panel was proposing to make it easier for counterintelligence and law enforcement entities to "deter, detect and prosecute" espionage cases through stiffer Top Secret clearance checks, polygraph tests and new penalties for "espionage-related activities."

The 13 ways to improve counterintelligence recommended by the panel were:

1. Require people with top secret clearances to grant investigators access to financial, consumer credit and commercial records.

2. Amend privacy laws to allow unlimited access to financial records of top secret clearance holders.

3. Require government code and communications specialists and manufacturers of code machines to undergo regular polygraph examinatons.

4. Permit the National Security Agency to help former employees financially so that they have no need to obtain money by spying.

5. Amend espionage laws to make it a crime to possess espionage equipment with intent to spy.

6. Amend espionage laws to make the sale of top secret documents a crime, without having to disclose the information contained in the documents.

7. Amend espionage laws to make it a crime to remove top secret documents from secure areas.

8. Expand laws requiring forfeiture of profits obtained from crime to include espionage.

9. Amend federal retirement laws to permit the government to deny retirement pay to people convicted of espionage in foreign courts when U.S. secrets are involved.

10. Amend consumer law to permit the FBI to obtain consumer reports on people suspected of being foreign agents.

11. Amend privacy laws to permit FBI access to unlisted telephone numbers of suspected foreign agents.

12. Amend law to permit offering up to $1 million rewards for information about espionage.

13. Amend surveillance law to create a process for obtaining court orders for physical searches in national security cases.

Senator Boren said espionage cases "continue to surface with disturbing frequency." Despite the changes occurring in the Soviet Union and Eastern Europe, Boren noted that the United States has not seen a decrease in hostile spying, instead, "we have seen an increase in espionage activities."

Both Senator Boren and Senator Cohen indicated that economic espionage will be the big problem in the future. Senator Boren stated that although the KGB was trying to improve its public image by showing a less aggressive intelligence service, the KGB Chairman Vladimir Kryuchkov indicated "in simple terms, espionage against commerical targets will become the great equalizer for the shortcomings of the Soviet economy."

Senator Cohen said, "The era of the cloak and dagger may be over, but the cloaks are likely to multiply and become even more pervasive in their effort to procure military, industrial, and commercial secrets."

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release *September 13, 1993*

EXECUTIVE ORDER
12863

PRESIDENT'S FOREIGN INTELLIGENCE ADVISORY BOARD

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the security of the United States by improving the quality and effectiveness of intelligence available to the United States, and to assure the legality of activities of the Intelligence Community, it is ordered as follows:

Part I. Assessment of Intelligence Activities

Section 1.1. There is hereby established, within the White House Office, Executive Office of the President, the President's Foreign Intelligence Advisory Board (PFIAB). The PFIAB shall consist of not more than 16 members, who shall serve at the pleasure of the President and shall be appointed by the President from among trustworthy and distinguished citizens outside the Government who are qualified on the basis of achievement, experience and independence. The President shall establish the terms of the members upon their appointment. To the extent practicable, one-third of the PFIAB at any one time shall be comprised of members whose term of service does not exceed 2 years. The President shall designate a Chairman and Vice Chairman from among the members. The PFIAB shall utilize full-time staff and consultants as authorized by the President. Such staff shall be headed by an Executive Director, appointed by the President.

Sec. 1.2. The PFIAB shall assess the quality, quantity, and adequacy of intelligence collection, of analysis and estimates, and of counterintelligence and other intelligence activities. The PFIAB shall have the authority to review continually the performance of all agencies of the Federal Government that are engaged in the collection, evaluation, or production of intelligence or the execution of intelligence policy. The PFIAB shall further be authorized to assess the adequacy of management, personnel and organization in the intelligence agencies. The heads of departments and

The Jacobs Panel

Eli Jacobs: Baltimore Orioles owner. He was a Reagan-era arms control advisor; and sat on Pentagon advisory panels.

Richard Helms: former Director of Central Intelligence.

Lloyd Cutler: former Carter White House counsel.

Arthur Culvahouse: former Reagan White House counsel.

Seymour Weiss: former ambassador and top Department of State official.

Sol Linowitz: former Xerox executive, ambassador and Mid-East negotiator.

Warren Christopher: former deputy Secretary of State.

Harold Edgar: Columbia University professor; espionage law expert.

agencies of the Federal Government, to the extent permitted by law, shall provide the PFIAB with access to all information that the PFIAB deems necessary to carry out its responsibilities.

Sec. 1.3. The PFIAB shall report directly to the President and advise him concerning the objectives, conduct, management and coordination of the various activities of the agencies of the Intelligence Community. The PFIAB shall report periodically, but at least semiannually, concerning its findings and appraisals and shall make appropriate recommendations for the improvement and enhancement of the intelligence efforts of the United States.

Sec. 1.4. The PFIAB shall consider and recommend appropriate action with respect to matters, identified to the PFIAB by the Director of Central Intelligence, and the Central Intelligence Agency, or other Government agencies engaged in intelligence or related activities, in which the advice of the PFIAB will further the effectiveness of the national intelligence effort. With respect to matters deemed appropriate by the President, the PFIAB shall advise and make recommendations to the Director of Central Intelligence, the Central Intelligence Agency, and other Government agencies engaged in intelligence related activities, concerning ways to achieve increased effectiveness in meeting national intelligence needs.

Part II. Oversight of Intelligence Activities

Sec. 2.1. The Intelligence Oversight Board (IOB) is hereby established as a standing committee of the PFIAB. The IOB shall consist of no more than four members appointed from among the membership of the PFIAB by the Chairman of the PFIAB. The Chairman of the IOB shall be appointed by the Chairman of the PFIAB. The Chairman of the PFIAB may also serve as Chairman of the IOB. The IOB shall utilize such full-time staff and consultants as authorized by the Chairman of the PFIAB.

Sec. 2.2. The IOB shall:

(a) prepare for the President reports of intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive;

(b) forward to the Attorney General reports received concerning intelligence activities that the IOB believes may be unlawful or contrary to Executive order or Presidential directive;

(c) review the internal guidelines of each agency within the Intelligence Community that concern the lawfulness of intelligence activities;

(d) review the practices and procedures of the Inspectors General and General Counsel of the Intelligence Community for discovering and reporting intelligence activities that may be unlawful or contrary to Executive order or Presidential directive; and

(e) conduct such investigations as the IOB deems necessary to carry out its functions under this order.

Sec. 2.3. The IOB shall, when required by this order, report to the President through the Chairman of the PFIAB. The IOB shall consider and take appropriate action with respect to matters identified by the Director of Central Intelligence, the Central Intelligence Agency or other agencies of the Intelligence Community. With respect to matters deemed appropriate by the President, the IOB shall advise and take appropriate recommendations to the Director of Central Intelligence, the Central Intelligence Agency or other agencies of the Intelligence Community.

Sec. 2.4. The heads of departments and agencies of the Intelligence Community, to the extent permitted by law, shall provide the IOB with all information that the IOB deemed necessary to carry out its responsibilities. Inspectors General and General Counsel of the Intelligence Community, to the extent permitted by law, shall report to the IOB, at least on a quarterly basis and from time to time as necessary or appropriate, concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive order or Presidential directive.

Part III. General Provisions

Sec. 3.1. Information made available to the PFIAB, or members of the PFIAB acting in their IOB capacity,

shall be given all necessary security protection in accordance with applicable laws and regulations. Each member of the PFIAB, each member of the PFIAB's staff and each of the PFIAB's consultants shall execute an agreement never to reveal any classified information obtained by virtue of his or her services with the PFIAB except to the President or to such persons as the President may designate.

Sec. 3.2. Members of the PFIAB shall serve without compensation but may receive transportation expenses and per diem allowances as authorized by law. Staff and consultants to the PFIAB shall receive pay and allowances as authorized by the President.

Sec. 3.3. Executive Order No. 12334 of December 4, 1981, as amended and Executive Order No. 12537 of October 28, 1985, as amended, are revoked.

WILLIAM J. CLINTON
THE WHITE HOUSE

September 13, 1993.

President, Bill Clinton

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA
v. Criminal No. 94-64-A
ALDRICH HAZEN AMES,
A/K/A "Kolokol",
a/k/a "K"

STATEMENT OF FACTS

In the event that this matter were to proceed to trial, the government would prove the following beyond a reasonable doubt:

I. INTRODUCTION

ALDRICH HAZEN AMES is 52 years old, born on May 26, 1941. In June 1962, ALDRICH HAZEN AMES accepted employment with the Central Intelligence Agency (CIA) of the United States, and he has been a full-time CIA employee for more than 31 years. At the time of his arrest, AMES was a GS-14 Operations Officer in the Counternarcotics Center at CIA Headquarters in Langley, Virginia.

During his employment with CIA, AMES held a variety of positions including the following: from 1983 to 1985, AMES was the Chief, Soviet Operational Review Branch in the Operational Review and Production Group of the Soviet/East European (SE) Division of the Directorate of Operations (DO) of the CIA; from 1986 through 1989, AMES was assigned to the United States Embassy in Rome, Italy; from September 1989 through December 1989, AMES was Chief, Europe Branch, External Operations Group, SE Division; from December 1989 through August 1990, AMES was the Chief, Czechoslovak Operations Branch, East European Operations Group, SE Division; from September 1990 through August 1991, AMES was assigned to the USSR Branch, Analytical Group, Counterintelligence Center; from September 1991 through November 1991, AMES was Chief, KGB. [1] Working Group, Central Eurasia (CE) Division; from December 19091 through August 1993, AMES was a

referant for CE Branch, regional Programs Branch, International Counternarcotics Group, Counternarcotics Center (ICG/CNC) and from August 1993 to February 1994, AMES was Chief, Europe and CE Branch, ICG/CNC. Throughout AMES' employment with the CIA, he held a TOP SECRET security clearance and had regular access to information and documents classified SECRET and TOP SECRET pursuant to Executive Order 12356.

On August 10, 1985, AMES married Maria del Rosario Casas Dupuy in the Commonwealth of Virginia. Prior to their arrests on February 21, 1994, ALDRICH and ROSARIO AMES resided at 2512 North Randolph Street, Arlington, Virginia, in the Eastern District of Virginia, with their minor son.

II. ESPIONAGE RELATED ACTIVITIES

In 1984, as part of his duties as a CIA Operations Officer, ALDRICH HAZEN AMES began meeting with officials of the Embassy of the Union of Soviet Socialist Republics ("U.S.S.R." or "Soviet Union." in Washington, D.C. These meeting were authorized by the Central Intelligence Agency and the Federal Bureau of Investigation, and were designed to allow AMES to assess Soviet officials as possible sources for intelligence information and recruitment. AMES was required to report each of his meetings with these Soviet officials to CIA officials.

In approximately April 1985, AMES agreed with Soviet officials to sell classified information from the Central Intelligence Agency and other branches of the United States government to the KGB, in return for large sums of money. In May and July 1985, AMES engaged in authorized meetings with Soviet officials, meetings he used as a cover to provide classified information to the KGB in exchange for money. Although AMES stopped regularly reporting these meetings to the CIA in July 1985, over the next year AMES continued to meet with the KGB in Washington, D.C. During many of these meetings, AMES provided classified information relating to the national defense of the United States to the KGB in return for cash payments.[2]

In July 1986, ALDRICH HAZEN AMES was assigned to the United States Embassy in Rome, Italy, where he served until July 1989. During this time, AMES met with his KGB handler, codenamed "SAM." AMES reported a few of these meetings to the CIA, claiming that he was obtaining information from "SAM," a Soviet Embassy official. During these meetings, AMES continued to disclose classified information relating to the national defense of the United States which AMES obtained through his work for the CIA in Rome.

In the Spring of 1989, as AMES was preparing to return to CIA Headquarters in Langley, Virginia, the KGB provided him with two written documents. The first document was a financial accounting which indicated that as of May 1, 1989, AMES had already receive approximately $1.8 million and that some $900,000 more had been appropriated for him. The

Aldrich Hazen Ames

second document was a nine-page letter which listed the types of classified information the KGB wanted AMES to obtain for them upon his return to CIA Headquarters,[3] discussed arrangements for cash payments to AMES upon his return to the United States, warned AMES to avoid traps set by the CIA, and detailed a communication plan governing further communications between AMES and the KGB. Pursuant to this communication plan, AMES would pass documents to and receive money from the KGB in the Washington, D.C. area at set times throughout the year using signal sites and dead drops. AMES would also meet personally with the KGB at least once yearly in meetings outside the United States. The fixed site for these meeting would be in Bogota, Colombia, on the first Tuesday every December, although additional meetings could be held in other cities, including Vienna, Austria, on an as needed basis.

In 1990, the KGB provided AMES with a communications plan for 1991 through a dead drop in the Washington, D.C. area. The 1991 communication plan provided for impersonal contacts through signal sites and dead drops, and for personal meetings between AMES and the KGB in Vienna, Austria, in April, and in Bogota, Colombia, in December. On December 17, 1990, AMES obtained valuable intelligence information regarding a KGB officer cooperating with the CIA. AMES prepared a letter for the KGB on his home computer advising the KGB of this information and the cryptonym of the KGB officer.

Pursuant to AMES' communication schedule with the KGB, on April 25, 1991, AMES traveled to Vienna, Austria, to meet with his KGB handlers. Although AMES was present in Vienna and prepared to exchange classified information for money, the KGB failed to meet with AMES at that time. Later that year, in December 1991, AMES met personally with the KGB in Bogota, Colombia, where he exchanged classified information for a large amount of cash. At that meeting, the KGB provided AMES a communications plan for 1992, pursuant to which they would communicate through signal sites and dead drops in March and August, and meet personally in Caracas, Venezuela, in October of 1992.

One of Ames' dead drop sites.

In March 1992, defendant ALDRICH HAZEN AMES communicated with the KGB by placing a signal at signal site SMILE and leaving a message with a package of documents at dead drop BRIDGE. In this message to the KGB, AMES requested that they promptly transmit more money to him through a dead drop. Again in June, 1992, AMES prepared a message on his computer to the KGB in which he complained of their failure to provide him money in response to his previous message, indicated that he was forced to sell stocks and certificates of deposit in Zurich to meet pressing needs, and asked them to deliver to him up to $100,000 in cash through dead drop PIPE. This message was transmitted to the KGB by placing a signal at signal site SMILE and leaving the message at dead drop BRIDGE.

On August 18, 1992, AMES typed a letter to the KGB on his home computer, at his home in the Eastern District of Virginia, discussing dead drops and his access to classified information, stating: "My lack of access frustrates me, since I would need to work harder to get what I can to you. It was easier to simply hand over cables! Documents are enclosed in this package which should be of interest."

In discussing his possible transfer to a different position within the CIA, AMES stated that, "If this job offer becomes serious during the next week or so, I will surely take it. It would be more interesting and productive for us." In this letter, AMES agreed to a personal meeting with the KGB in Caracas, Venezuela and AMES also provided them with information on the level of CIA operations in Moscow, U.S. conclusions about Russian technical penetrations of our embassy in Moscow, and CIA recruitment plans for Russian officials. The letter also stated that, "My wife has

accomodated (sic) herself to understanding what I am doing in a very supportive way."

AMES attempted to transmit this letter and accompanying classified documents to the KGB on August 19, 1992, by placing a pencil mark at signal site HILL in the morning and thereafter leaving the documents and letter at dead drop GROUND at 4 p.m. that day. Early the next day, however, AMES returned to the signal site and determined that his signal to the KGB had not been erased, signifying that they had not picked up his package from the dead drop. AMES thereafter retrieved his package, and on September 1, 1992, typed a second letter to the KGB on his home computer. This letter advised them that he had been forced to retrieve his earlier drop and would signal them again. This message, along with the earlier package, was retransmitted to the KGB in early September through dead drop GROUND.

On October 2, 1992, pursuant to his communications plan, AMES traveled to Bogota, Colombia, and then on to Caracas, Venezuela, to meet with officers of the KGB. During this meeting, AMES provided the KGB with classified information and received in return approximately $150,000 in cash. The KGB also provided AMES with a communications plan for 1993, pursuant to which AMES would transmit information and messages to them by dead drops in January, April, July, and October, receive money and messages from the KGB in March, June, and September, and would meet with them personally in Bogota, Colombia, in November or December 1993. Upon his return to the United States, AMES deposited more than $85,000 of the KGB money received in Caracas into accounts he controlled with his wife in banks in Northern Virginia, all deposits in amounts of less than $10,000.

One of Ames' signal sites.

On March 9, 1993, AMES typed a message to the KGB on his home computer discussing a variety of topics including the morale of the CIA division concerned with the former U.S.S.R and Russia, personnel changes and budgetary matters in the CIA, and the fact that he was transmitting to them a "variety" of documents. AMES opened this message telling the KGB, "All is well with me—I have no indications that anything is wrong or suspected." This message, along with a package of classified documents and information, was transmitted to the KGB through a dead drop in March 1993.

On May 26, 1993, AMES transmitted an "urgent" message to the KGB, asking for money to be delivered to him immediately through a dead drop in the Washington, D.C. area. Four days later, the KGB transmitted a package containing a substantial amount of cash to AMES through dead drop BRIDGE. In July 1993, the KGB transmitted to AMES additional money through a dead drop, as well as a message discussing an upcoming personal meeting, and their plan to test a dead drop to determine whether it was secure. In this message, the KGB advised AMES that they would provided additional money shortly, unless the money was postponed due to the "diplomatic pouch schedule."

In preparation for his trip to Bogota on September 8, 1993, AMES drafted a message to the KGB stating that he would be available to meet with them on October 1, 1993. On September 9, 1993, AMES left this message for the KGB, and that evening drove with his wife into the District of Columbia to determine whether the KGB had received the message. Later that month, the KGB signaled AMES through signal site NORTH, advising him they would be unavailable to meet with him on October 1, 1993, and transmitted a message to him through dead drop PIPE stating they would meet with him between November 1 and November 8, 1993. On October 18, 1993, AMES signaled his willingness to attend this meeting in Bogota by placing a chalk mark at signal site SMILE.

Thereafter, on October 30, 1993, AMES traveled to Bogota, Colombia, where he met with officers of the KGB. In Bogota, AMES provided the KGB with classified information in exchange for a substantial amount of cash. In Bogota, AMES also received a communications plan for 1994 which established new signal sites throughout the Washington metropolitan area and provided for dead drops in February, March, May, August, and September, face-to-face meetings in Caracas, Venezuela, or Quito, Ecuador, in November 1994, and a face-to-face meeting in 1995 in either Vienna, Austria, or Paris, France. During this meeting, the KGB also advised AMES that they were holding $1.9 million for him.

III. COMPROMISE OF CLASSIFIED INFORMATION

When ALDRICH HAZEN AMES began spying for the KGB in the Spring of 1985, his position within the CIA guaranteed him access to most information relating to penetrations of the Soviet military and intelligence services and intelligence operations against the Soviet Union. AMES disclosed substantial amounts of this information, including the identities of Russian military and intelligence officers who were cooperating with the CIA and friendly foreign intelligence services, including but not limited to, sources codenamed GTACCORD, GTCOWL, GTFITNESS, GTBLIZZARD, GTGENTILE, GTMILLION, GTPROLOGUE, GTWEIGH, GTTICKLE, and others.[4] AMES' disclosures included a substantial amount of TOP SECRET information including signals intelligence. AMES' compromise of these penetrations of the Soviet military and intelligence services deprived the United States of extremely valuable intelligence material for years to come.

During his assignment to the U.S. Embassy in Rome from 1986 to 1989, AMES provided the KGB with valuable intelligence information concerning CIA activities against the Soviet Union, including a large number of double agent operations launched against the Soviet Union. AMES compromised a substantial number of double agent operations organized by U.S. intelligence agencies, and also advised the KGB of our knowledge of Soviet double agent operations targeted against the U.S. AMES informed the KGB of important CIA strategies involving double agent operations and answered detailed inquiries regarding past penetrations of the Soviet intelligence services. During this period AMES also disclosed to the KGB the identities of an Eastern European security officer who had begun cooperating with the CIA, code named GMMOTORBOAT, and a soviet official cooperating with CIA, codenamed GTPYRRHIC.

Following his return in 1989 to CIA Headquarters, AMES continued to provide the KGB with valuable classified information related and unrelated to his specific CIA job assignments. AMES also provided the KGB with a substantial amount of information regarding CIA and other U.S. intelligence agencies, including information on budgets, staffing, personnel, morale, strategy, and other issues affecting the Soviet Union and Russia.

IV. THE FINANCES AND FALSE TAX RETURNS

During this conspiracy, defendant ALDRICH HAZEN AMES received approximately $2.5 million from the KGB for his espionage activities. AMES received this money primarily in face-to-face meetings overseas, but also through dead drops in the Washington, D.C. area. While AMES was stationed in Rome, he deposited the bulk of this cash into two accounts at Credit Suisse Bank in Zurich, Switzerland.[5] For example, on June 29, 1989, prior to departing Rome for the Untied States, AMES deposited a total of $450,00 in cash into two accounts he controlled at Credit Suisse.

AMES and his wife, Rosario Casas Ames, used the money received from the KGB to purchase a residence in Arlington, Virginia for $540,000, property in Colombia, expensive automobiles, extensive wardrobes, and to pay approximately one-half million dollars in credit card bills. A portion of the money was used to support Rosario Casas Ames' family in South America as well. Most of the money deposited in cash into United States banks was deposited in sums less than $10,000 to avoid having the financial institutions file a Currency Transaction Report.

Of the approximately $2.5 million paid to AMES by the KGB, none of the money was declared on AMES' United States income tax returns. ALDRICH HAZEN AMES subscribed and filed false Joint Income Tax Returns for tax years 1985, 1986, 1987, 1988, 1989, 1990, 1991, and 1992.

In committing the foregoing acts, ALDRICH HAZEN AMES acted knowingly, willfully, and unlawfully, not by accident or mistake.

Respectfully submitted,

HELEN F. FAHEY
UNITED STATES ATTORNEY

(NOTE: On 28 April 1994 Rick Ames was sentenced to life inprisonment.)

Central Intelligence Agency

Washington, D. C. 20505

Immediate Release *31 October 1995*

DIRECTOR OF CENTRAL INTELLIGENCE JOHN DEUTCH STATEMENT TO THE PUBLIC ON THE AMES DAMAGE ASSESSMENT

For the past year and a half, an independent team of Intelligence Community analysts and operations officers has conducted a Damage Assessment of the actions of Aldrich Ames, who, while a CIA Directorate of Operations officer from 1985 to 1994, committed espionage for Soviet (and later Russian) intelligence. This Damage Assessment, commissioned by my predecessor, is now complete. I testified before the House and Senate Permanent Select Committees on Intelligence on October 31st and laid out the findings and actions that I have put in place to remedy the shortcomings it identified.

The Ames case is one of those landmark events which defines the course of an organization. It requires some public discussion because the American people need to know that the Central Intelligence Agency has drawn the right lessons from the incident, and is moving determinedly to make fundamental changes which will reduce the chance that something like this will happen again. Smart organizations use every experience—whether good or bad — as motivation to improve. I am determined to use the Ames case as the basis for bringing bold management changes to the CIA.

I have provided the congressional intelligence oversight committees with details concerning the damage caused by Aldrich Ames' treachery. But let me describe a basic outline of the damage that was done, the weaknesses in the CIA which the incident revealed, and the corrective actions which have been and are being taken.

The damage which Aldrich Ames did to his country can be summarized in three categories:

— By revealing to the Soviet Union the identities of many assets who were providing information to the United States, he not only caused their executions, but also made it much more difficult to understand what was going on in the Soviet Union at a crucial time in its history;

— By revealing to the Soviet Union the way in which the United States sought intelligence and handled assets, he made it much more difficult for this country to gather vital information in other countries as well;

— By revealing to the Soviet Union identities of assets and American methods of espionage, he put the Soviet Union in the position to pass carefully selected "feed" material to this country through controlled assets;

The damage done by Aldrich Ames is documented in the Damage Assessment Report which I have submitted to the intelligence committees. I endorse the Report. I have also made this painstaking work of many months available to other agencies of government so that damage control actions can be taken.

While Ames damaged our intelligence activities in a number of areas, his betrayal of our most important assets is particularly egregious. In a single disclosure, he revealed the identities of CIA's most valuable Soviet/Russian assets.

The Report also revisits deficiencies in the organization, procedures, and management of the Central Intelligence Agency. These deficiencies fall into two major categories:

— The counterintelligence function in the CIA had become neglected by management compared to other

functions. It was poorly staffed and organized, and characterized by lax procedures. Its coordination with the Department of Justice was badly flawed by turf-tending and bureaucratic infighting.

— Most troubling of all was an important new finding of the Assessment, which is substantiated by a Special Inspector General Report I requested this summer, that consumers were not informed that some of the most sensitive human intelligence reporting they received came from assets that were known or suspected of being controlled by the KGB/SVR. This finding disturbs me greatly, and this deficiency is one of the first I have moved to correct.

These are the major issues underlying the damage done and the shortcomings that were revealed by Aldrich Ames' espionage activities, and are documented in the thorough report which has been submitted to the intelligence committees.

What is critically important in this incident is the future. What is the Central Intelligence Agency doing as a result of this incident, and its aftermath, to reduce the chance that this happens again?

My most urgent task is to re-establish credibility with our consumers. I will establish a new, independent Customer Review Process for sensitive human reporting that will be managed by the National Intelligence Council. Both the Directorate of Operations and our customers agree with this mechanism to improve customer knowledge without excessive intrusion into operations.

When I took office six months ago, I found that many corrective actions in the wake of the Ames case were underway, well documented in a strategic plan for change. I have taken additional actions in my time as Director of Central Intelligence, particularly in the areas of personnel, organization, and accountability.

DCI, John Deutch

The major categories of the corrective actions and improvement are these:

— A major changeover in the management of the Central Intelligence Agency, including the replacement of the top three levels of Agency management and much of the fourth level with new leadership committed to change. This new management team includes a new Deputy Director for Operations, as well as Associate Deputy Directors for Operations, Counterintelligence, and Human Resources, and seven Directorate of Operations component chiefs.

The Ames Notebook

Ames passed the names of two CIA officers, who were handling compromised CIA agents, to the KGB in an effort to throw suspicion on them for the loss of American intelligence penetrations of the Soviet Union.

In an endeavor to be promoted, Ames asked the KGB to provide a Russian spy for him to recruit but the KGB denied his request as too risky.

The KGB changed their dead drop modus operandi after Ames gave them an FBI report on Soviet intelligence dead drop methodology. For the first time, the KGB used public parks to clear dead drops and to communicate with Ames.

Despite missing three personal meetings because of drunkenness, Ames met with the KGB 11 times between 1985 and 1993. The KGB recorded the 40 hours Ames spent with them.

The KGB expressed interest in their former republics and asked Ames about CIA operations in these areas and if CIA communicated directly with agents there.

The KGB asked Ames about a suspected KGB officer in Vienna, Austria.

After the Soviets advised Ames that they had set aside $2 million for him, he attempted to have the money transferred to his bank account in the United States. The Soviets refused fearing he might stop spying for them.

Ames never considered living on the property the KGB arranged for him in Moscow; instead he thought about retiring in southern France or Colombia.

—The establishment of the National Counterintelligence Center at CIA, headed by a senior FBI officer;

—Significantly increasing the application of counterintelligence to operations, and emphasizing counterintelligence awareness and training in all activities;

— New guidelines for Agency managers on handling employee suitability issues and strengthening internal discipline procedures;

— Policies to ensure that new emphasis is placed on the quality of agent recruitment and agent handling, rather than on the quantity of recruitment. This includes a complete scrubbing of standards and criteria for personnel evaluation as well as a system of rewards that moves away from quantity to quality in asset recruitment as the prime measure of success;

— A revitalized system within the Directorate of Operations to validate assets, bringing in a team approach involving analysts and counterintelligence officers from the very beginning of cases;

— Clearly defined standards and expectations for the performance of Chiefs of Station along with a clearly defined policy for their selection;

— Initiatives aimed at improving the Agency's records management system and bolstering computer security; and,

— Perhaps most important, insistence from the top down on integrity and accountability in the Central Intelligence Agency. This includes the establishment of component-level accountability boards within the Directorate of Operations and a senior Directorate-level accountability board.

I also considered the accountability of certain CIA officers in connection with the Damage Assessment Team Report and the Inspector General Report on the same subject. In making my determinations I applied the following standards:

— That the performance deficiency at issue must be specific;

— That, unlike military practice, the individual being held accountable must have had a direct responsibility and role—that is, the individual, by virtue of his/her position, had the opportunity or responsibility to act; and,

— That high levels of professionalism are required.

The Inspector General, in the special report provided to me last month, recommended 12 CIA officers be held responsible for their roles in this matter. All but one of those individuals has retired, thereby restricting my options for disciplinary action. Based on the information in the Damage Assessment Team Report as well as the IG report, if these officers were still employed, I would have dismissed two individuals from CIA and taken no disciplinary action against five. I have reprimanded the one officer who is currently employed. As for the two I would have dismissed, both now are banned from future employment with the Agency. Four other former officers have been given reprimands or warnings.

I want to emphasize that the Ames Damage Assessment, in all of its detail, does nothing to shake my conviction that we need a clandestine service. Of all the intelligence disciplines, human intelligence is, indeed, the most subject to human frailty, but it also brings human intuition, ingenuity, and courage into play against the enemies of our country. Often there is no other way to penetrate a terrorist cell or a chemical weapons factory or the inner circle of a tyrant. At critical times human intelligence has allowed our leaders to deal with the plans and intentions—rather than the weapons—of our enemies.

I believe that the right actions are underway for the Ames incident to become the most powerful catalyst for change in the history of the Central Intelligence Agency. The key is drawing unflinchingly the right lessons and making the necessary changes. It will take time to implement all these reforms and accomplish required changes to some aspects of the CIA's habits, practices, and attitudes. The United States must have the best intelligence capability in the world, and that capability includes the Operations Directorate of the Central Intelligence Agency.

The Directorate of Operations must be staffed by top-notch people. This means that first-class people are hired, their careers are managed properly, and the promotion system rewards those who maintain the highest standards of integrity, but also who are prepared to take risks. By clearly defining the rules and management expectations, we will encourage these officers to take the risks necessary to produce the critical intelligence needed by our Nation.

It must have solid procedures which ensure a quality product for decision-makers throughout government. This means emphasizing quality and authenticity over numbers and volume. This also means that safeguards against false information are comprehensive and effective.

I believe that the changes which were taken before my watch, and the additional measures I have taken—coupled with the desire for fundamental, positive change by the overwhelming majority of CIA officers themselves— ensure that we are on the right track.

Statement of the Director of Central Intelligence on the Clandestine Services and the Damage Caused by Aldrich Ames

7 December 1995

Introduction and Overview

From the earliest days of the Republic, the United States has recognized the compelling need to collect intelligence by clandestine means. For much of our history, this collection could only be done by human agents. Recent technological developments have, of course, vastly increased our ability to collect intelligence. The capacity of these technical systems is awesome and our achievements are astonishing. However, these technical means can never eliminate the need for human sources of information. Often, the more difficult the target is, the greater is the need for human agents.

Throughout our history, the contribution of the clandestine service of the United States has frequently been the difference between victory and defeat, success and failure. It has saved countless American lives.

In recent years, human agents have provided vital information on military and political developments in the Soviet Union, terrorist groups, narcotics trafficking, development of weapons of mass destruction and other grave threats to the United States. These agents often provided the key piece of information that formed the United States' understanding of a critical international situation.

For decades, information from human agents inside the Soviet Union gave us vital insights into the intentions and capabilities of the Soviets. Ames clearly dealt a crushing blow to those efforts. Nonetheless, I am convinced that when the full history of the Cold War is written, American intelligence-and human intelligence in particular-will be recognized as having played an important role in winning that war.

It must be remembered that for over forty years the United States faced a hostile state with enormous nuclear power. A misstep by either side could have destroyed the world. That nuclear war did not occur and that the Soviet Union ultimately collapsed is in no small part attributable to the brave, tireless and too often thankless efforts of the clandestine intelligence service of the United States. The DCI has a great responsibility to preserve and nurture this vital capability.

That said, it must be pointed out that while human agent operations have the potential for high gain, they also entail high risk. Human agent operations are almost always in violation of another country's laws. It is therefore imperative that they be subject to tight policy control and carried out within the scope of American law. These operations must be carried out in secret, for secrecy is vital to success.

The American public is often troubled by activities that are done in secret. This is a natural and healthy instinct. It has served our democracy extremely well for over two hundred years. However, I believe the American people understand the need for secrecy in human agent operations. They agree with a letter written by George Washington when he was Commander-in-Chief of the Continental Army in the summer of 1977:

"The necessity of procuring good intelligence is apparent & need not be further urged-All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, Success depends in Most Enterprises of the kind, and for want of it, they are generally defeated, however well planned & promising a favorable issue."

The American people will accept secret intelligence activity only if four conditions are met. First the acts must be consistent with announced policy goals. Second, they must be carefully controlled under U.S. law. Third, the operations should be consistent with basic American values and beliefs. And fourth, when American intelligence services make mistakes—as we have and will surely do again—we learn from those mistakes.

Because much of what the intelligence services do is secret, Congressional oversight is the key to providing the American people the confidence that their intelligence services are meeting these four conditions. Indeed Congressional oversight is the best way this confidence can be assured.

We must not quit simply because we have made errors, even serious ones. The need for effective intelligence is too important. We must constantly learn from our mistakes, make the necessary changes, and continue to take the risks necessary to collect vital intelligence so urgently needed by the President, the Congress, and other senior policy-makers.

With this in mind, we have moved quickly to strengthen the capabilities of the clandestine service across a broad spectrum. Counterintelligence programs have been significantly enhanced, tradecraft techniques are being tailored for the world in which we now live, and the technologies needed for the future are being rapidly developed. Underpinning these efforts has been a renewed emphasis on quality management that pays attention not only to what we do, but how we do it. All these initiatives, imbedded in a strategic plan developed by the clandestine service this past year, position the clandestine service to meet our future challenges.

The Actual Damage

On the 31st of October, I appeared before the House and Senate Intelligence Committees in closed session to describe the results of the Ames damage assessment commissioned by my predecessor, Jim Woolsey. Following that testimony, we have continued to review

the report of the Damage Assessment Team (DAT) and to consult with both Committees, the Department of Defense, the Department of State and other interested agencies. Accordingly, I believe it is appropriate to report to you on our continuing review and our consultation with other agencies. I also believe it is important that additional information be made available to the American public so that they can understand the nature and extent of the damage caused by Ames. (It should also be recalled that in the 1980's, the U.S. experienced a number of other espionage cases. Edward Lee Howard, an agency officer, like Ames, caused considerable damage to US HUMINT Operations against the USSR. John Walker and Ronald Pelton caused immense damage to US interests. (In Walker's case, vast amounts of information on our military capabilities and plans were exposed which could have had tragic consequences in the event of war.) I have attached a copy of the public statement that I issued on the 31st of October. Let me add some detail on the scope of the damage.

Aldrich Ames' espionage on behalf of the Soviet Union and Russian from April 1985 through February 1994 caused severe, wide-ranging and continuing damage to US national security interests. In addition to the points that I made in my public statement on 31 October, Ames did the following:

In June 1985, he disclosed the identity of numerous U.S. clandestine agents in the Soviet Union, at least nine of whom were executed. These agents were at the heart of our effort to collect intelligence and counterintelligence against the Soviet Union. As a result, we lost opportunities to better understand what was going on in the Soviet Union at a crucial time in history.

He disclosed, over the next decade, the identity of many US agents run against the Soviets, and later the Russians.

He disclosed the techniques and methods of double agent operations, details of our clandestine tradecraft, communications techniques and agent validation methods. He went to extraordinary length to learn about U.S. double agent operations and pass information on them to the Soviets.

He disclosed details about US counterintelligence activities that not only devastated our efforts at the time, but also made us more vulnerable to KGB operations against us.

He identified CIA and other intelligence community personnel. Ames contends that he disclosed personal information on, or the identities of, only a few American intelligence officials. We do not believe that assertion.

He provided details of US intelligence technical collection activities and analytic techniques.

He provided finished intelligence reports, current intelligence reporting, arms control papers, and selected Department of State and Department of Defense cables. For example, during one assignment, he gave the KGB a stack of documents estimated to be 15 to 20 feet high.

Taken as a whole, Ames' activities also, facilitated the Soviet, and later the Russian, effort to engage in "perception management operations" by feeding carefully selected information to the United States through agents whom they were controlling without our knowledge. Although the extent and success of this effort cannot now be determined with certainty, we know that some of this information did reach senior decision-makers of the United States.

As the Committee knows, one of the most disturbing findings of the DAT was that consumers of intelligence were not informed that some of the most sensitive human intelligence reporting they received came from agents known or suspected at the time to be under the control of the KGB, and later the SVR. This finding was substantiated by a detail audit done by the CIA's Inspector General. Because this aspect of the assessment is so important and has generated so much public interest, I would like to discuss it in some detail.

In response to requests from the DAT, some consumers of sensitive human reporting identified just over 900 reports from 1985 to 1994 that they considered particularly significant. These consumers included CIA's Directorate of Intelligence, the Defense Intelligence Agency, the National Security Agency, the Military Services and other agencies. The DAT then reviewed the case files of the agents who were the source

of just over half of these reports and conclude that a disturbingly high percentage of these agent were controlled by the KGB, and later the SVR, or that evidence exists suggesting that they were controlled.

Although some of the reports from these sources were accompanied by warnings that the source might be suspect, many other reports did not include adequate warning. The IG was asked to review reporting from the sources that the DAT concluded were known or suspected to be controlled. They concluded that CIA did not provide adequate warning to consumers of 35 reports from agents whom we have good reason to believe at the time were controlled and 60 reports from agents about whom we had suspicions at the time. Of these 95 reports, at least three formed the basis of memoranda that went to the President: one of those reports was from a source who we had good reason to believe was controlled.

The DAT intended to review the source of each of these reports but, for a variety of reasons, was not able to do so. For example, the filing system of the DO was incomplete and the sources for some reports could not be identified. To expedite the review, the DAT did not review the files of sources who produced only one or two reports. In the end, the Team examined and thoroughly reviewed the sources who produced roughly 55% of the reports cited by consumers as significant suspicions. While these and other reports could well have been reflected in other such analytic products, we have not identified them.

The fact that we can identify only a relatively few significant reports that were disseminated with inadequate warning does not mitigate the impact of Ames' treachery or excuse CIA's failure to adequately warn consumers. We believe that, whatever the numbers of such reports, the provision of information from controlled sources without adequate warning was a major intelligence failure that calls into doubt the professionalism of the clandestine service and the credibility of its most sensitive reporting.

The situation requires us to take two steps. First, and most importantly, we must ensure that such information does not reach senior policy-makers in the future without adequate warning that the information comes from sources we know or suspect to be controlled. Second, we must examine certain important decisions taken by the United States to ensure that they were not influenced by these reports. If any decisions were influenced by faulty reports, we must determine what, if any, corrective measures should be taken.

With respect to the first step, I have established a new Customer Review Process under the National Intelligence Council. This process, which will include appropriately cleared representatives to our customer agencies, will work with the Directorate of Operations to ensure that recipients of extremely sensitive human intelligence reports are adequately advised about our knowledge of the source of the reports. This does not mean that these representatives of other agencies will be told the identity of the source of the information. Rather, our goal is that recipients of especially sensitive information can adequately understand and evaluate the intelligence.

With respect to the second step-reviewing decisions that might have been made using controlled information— it is important to understand that our knowledge of the details of a Soviet perception management effort is limited, as is what can be said publicly about the subject. Also, it is not the job of the DCI to review decisions made by other agencies. However, it is very likely that the KGB and later the SVR, sought to influence U.S. decision-makers by providing controlled information designed to affect R&D and procurement decisions of the Department of Defense. The DAT believes one of the primary purposes of the perception management program was to convince us that the Soviets remained a superpower and that their military R&D program was robust.

In an effort to understand the impact of this Soviet/Russian program, the DAT reviewed intelligence reporting relevant to a limited number of acquisition decisions taken by the Department of Defense to determine whether any reports from controlled or suspect agents had an impact on the decisions. The reporting covered eight categories of weapon systems, including aircraft and related systems, ground force weapons, naval force weapons, air defense missiles and cruise missiles. The DAT concluded, in coordination with DIA and the intelligence components of the military departments, that the impact varied from program to program. In some cases the impact was

negligible. In other cases, the impact was measurable, but only on the margin.

The dissemination of reports on Soviet/Russian military R&D and procurement programs from questionable sources had the potential to influence U.S. military R&D and procurement programs costing billions of dollars. The DAT surveyed a number of intelligence consumers in the Department of Defense. They found that consumers were often reluctant to state that this reporting had any significant impact. Determining damage always involves much speculation, but the team concluded that "clear cut damage" to intelligence analysis may have been limited to a "few cases." They cited three in particular:

A report in the late 80's that would have influenced debates on U.S. general purpose forces,

Analyses of Soviet plans caused us to revise logistics support and basing plans in one overseas theater (see also above), and

Studies of certain Soviet/Russian cruise missile and fighter aircraft R&D programs may have overestimated the pace of those programs.

In addition, the team reviewed intelligence reporting that supported decisions in a number of defense policy areas, including U.S. military strategy. The team found that reporting from controlled or suspect agents had a substantial role in framing the debate. The overall effect was to sustain our view of the USSR as a credible military and technological opponent. The DAT found that the impact of such information on actual decisions, however, was not significant. In some cases, our military posture was altered slightly. In one example, changes already underway to enhance the survivability and readiness of the basing structure in an overseas theater was justified by information received from a controlled source. However, before the changes could be fully carried out, the Soviet Union collapsed, obviating the need for the change.

The DAT also reviewed a handful of national security issues that were the most likely to have been impacted by Ames' actions. For example, Ames passed U.S. all-source analysis of Soviet motives and positions in arms control negotiations. His espionage assisted their efforts to feed us information that supported the Soviet positions. The DAT interviewed a limited number of officials with respect to arms control issues and related programs. The DAT found no major instance where Soviets maneuvered U.S. or NATO arms control negotiators into giving up a current or future military capability or agreeing to monitoring or verification provisions that otherwise would not have been adopted. This conclusion is buttressed by the fact that the Soviet's bargaining position grew increasingly weak as its economy deteriorated and Gorbachev struggled to maintain control.

After reviewing the DAT report, I believe it is incorrect to maintain that this reporting was completely irrelevant or completely determinate in U.S. weapon system decisions. The process by which U.S. weapons system development and acquisition decisions are made is complex and involves many considerations. These include technical feasibility, force modernization, life cycle cost, and industrial base considerations, as well as estimates of the near and long term threat. No single strand of intelligence information ever serves as the full justification for undertaking a large program.

The kind of impact that intelligence does have is:

Influencing the pace and timing of a development program to meet an anticipated threat. This is an influence at the margin of system acquisition.

Shaping the thinking of the technical and contractor community on the threat envelope facing a system under development.

Creating an impression, in combination with other information, of the status and vitality of an adversary's military R&D and procurement activities.

All of this affects the context in which U.S. acquisition decisions are made. I believe the net effect of the Soviet/Russian "directed information" effort was that we overestimated their capability. Why the Soviet/Russian leadership thought this was desirable is speculative.

A DoD team, working at the direction of the Deputy Secretary of Defense, recently completed the Department's review of the impact of directed reporting

on military policy, acquisition, and operations. That report has been briefed to the Secretary and Deputy Secretary of Defense and the Congress.

The combination of the loss of key human sources compromised by Ames, plus the directed information the KGB and SVR provided to the U.S. through controlled sources, had a serious impact on our ability to collect and analyze intelligence information. The DAT concluded that Ames' actions diminished our ability to understand:

> Internal Soviet development, particularly the views and actions of the hard liners with the respect to Gorbachev in the late 1980's;
>
> Soviet, and later Russian, foreign policy particularly Yeltsin's policies on non-proliferation and Russian involvement in the former CIS states; and
>
> The extent of the decline of Soviet and Russian military technology and procurement programs.

The Ames case—and the other espionage cases of the 80s—remind us that other issues must be addressed. These include the serious lack of adequate counter-intelligence during much of the 80s and early 90s. My predecessors, the Attorney General and the Director of the FBI have made great progress in repairing this extremely important function. We have continued to make progress, but much works remains to be done. I detailed in my statement of 31 October a number of steps that are underway to correct these serious problems.

I look forward to working with the Committees to ensure the adequate implementation of these measures. I assure you that my colleagues in the Intelligence Community are fully committed to achieving these important reforms.

Conclusions

I regret that I cannot discuss in public more detail about the actual damage done by Aldrich Ames. To do so would compound that damage by confirming to the Russians the extent of the damage and permit them to evaluate the success and failures of their activities. That I cannot do.

However, it is extremely important that we not underestimate the terrible damage done by Ames' treachery. It is impossible to describe the anger and sense of betrayal felt by the Intelligence Community. It reverberates to this day and has given all of us renewed motivation to do our jobs. Across the board, in all areas of intelligence activitie—from collection, to counter-intelligence, to security, to analysis and production, to the administrative activities that support the Community effort—we must renew our efforts to ensure that our activities are conducted with integrity, honesty, and the highest standards of professionalism. To do less is to fail.

I believe that the most important value the Intelligence Community must embrace is integrity—both personal and professional. We operate in a world of deception. It is our job to keep this nation's secrets safe and to obtain the secrets of other nations. We engage in deception to do our job and we confront deception undertaken by other nations.

But we must never let deception become a way of life. We must never deceive ourselves. Perhaps more than any other government agency, we in the CIA must have the highest standards of personal and professional integrity. We must be capable of engaging in deceptive activities directed toward other nations and groups while maintaining scrupulous honesty among ourselves and with our customers. We must not let the need for secrecy obscure the honest and accurate presentation of the intelligence we have collected or the analyses we have produced.

I believe we have approached the damage done by Ames with honesty and integrity. We have made the hard calls. We may have to make more. We have taken the steps necessary to discipline those responsible, to reduce the likelihood of such damage recurring and to begin to restore the confidence of our customers and the American people.

As I said at the beginning of this report, clandestine human operations remain vital to this country's security. They are often the most dangerous and difficult intelligence operations to conduct. But I want to assure the Congress and the American people that the American clandestine service will continue to conduct these operations and do so in the highest tradition of integrity,

courage, independence and ingenuity that have made our service the best in the world.

Unclassified Abstract of the CIA Inspector Generals Report on the Aldrich H. Ames Case

Preface to the Report from the IG

Procedurally, this has been an unusual report for the CIA IG to write. In the first instance, our inquiry was directly requested by the Chairman and Vice-Chairman of the Select Committee on Intelligence of the U.S. Senate in late February 1994—shortly after Aldrich H. Ames was arrested. Normally, our congressional oversight committees ask the Director of Central Intelligence to request an IG investigation. On this occasion their request was directed to the IG.

Second, the DCI chose to ask us to look into the Ames matter in phases after Ames' arrest for fear of disrupting the Ames prosecution. We were requested to inquire into the circumstances surrounding the CI investigation of the Ames betrayal:

> What procedures were in place respecting CIA counterespionage investigations at the time Ames volunteered to the Soviets in 1985;
>
> How well did they work; and
>
> What was the nature of CIA's cooperation with the FBI in this case.

On March 10, 1994, the DCI asked us to seek to determine if individuals in Ames' supervisory chain discharged their responsibilities in the manner expected of them and directed the Executive Director of CIA to prepare a list of Ames' supervisors during the relevant periods. The DCI also directed that awards and promotions for the individuals on the Executive Director's list be held in escrow pending the outcome of the IG investigation. I wish to state at this point that neither I nor any member of the team investigating the Ames case have viewed the DCI's escrow list. We wanted to be as completely unaffected by the names on the list as we could be in order to discharge our responsibility to advise the DCI objectively of possible disciplinary recommendations. As a precautionary measure, I did ask my Deputy for Inspections, who is otherwise uninvolved in the Ames investigation, to view the escrow list to advise of any individuals on it whom we might have failed to interview through inadvertence. That has been our only involvement with the escrow list.

Third, there was an unusual limitation placed on our inquiry at the outset caused by a desire on the part of the DCI, the Department of Justice and the U.S. Attorney in the Eastern District of Virginia to do nothing that would complicate the Ames trial. We willingly complied with these constraints, confining ourselves to background file reviews and interviews of non-witnesses until the Ameses pled guilty on April 28, 1994. The consequence has been that we have had to cover a great deal of ground in a short period of time to conduct this investigation in order to have a report ready for the DCI and the congressional oversight committees by September 1994. I am extremely proud of our 12-person investigative team.

Apart from the unusual procedures affecting this investigation, the Ames case presented several major substantive problems as well. This case raised so many issues of concern to the DCI, the oversight committees and the American people, that we have not chosen to tell the story in our normal chronological way. Instead, we have focused on themes: Ames' life, his career, his vulnerabilities. We have tried to discuss how counterespionage investigations have been conducted in CIA since the Edward Lee Howard betrayal and the Year of the Spy, 1985—in the context of this particular case. Necessarily, we have made analytical judgments about what we have learned—some of them quite harsh. We believe this is our job—not just to present the facts, but to tell the DCI, the oversight committees and other readers how it strikes us. We have the confidence to do this because we have lived with the guts of Ames's betrayal and his unearthing for countless hours and we owe our readers our reactions. In this sense our 12 investigators are like a jury—they find the facts and make recommendations to the DCI for his final determination. This investigative team, like a jury, represents the attitude of the intelligence professionals from whose ranks they are drawn and from whom they drew testimony—sometimes shocked and dismayed at what we've learned, often appreciative of the individual

acts of competence and courage, and always intrigued by the complexity of the Ames story.

In the end, the Ames case is about accountability, both individual and managerial. The DCI and the congressional oversight committees have made this the issue, but if they had not, we would have. As a postscript to my opening sentences, let me note that the CIA IG had begun to look into the Ames case on its own, even before the SSCI or the DCI had requested it, because we believe that the statute setting up our office requires it. The issue of managerial accountability has been one of this office's principal points of focus since its inception in 1990—and we have enjoyed mixed success in our reviews and recommendations to promote it.

Seeking to determine managerial accountability in the Ames case has not been an easy task. On the individual level, we have uncovered a vast quantity of information about Ames' professional sloppiness, his failure to file accountings, contact reports and requests for foreign travel on time or at all. We have found that Ames was oblivious to issues of personal security both professionally—he left classified files on a subway train- and in his espionage—he carried incriminating-documents and large amounts of cash in his airline luggage; he carried classified documents out of CIA facilities in shopping bags; and he openly walked into the Soviet Embassy in the United States and a Soviet compound in Rome. We have noted that Ames' abuse of alcohol, while not constant throughout his career, was chronic and interfered with his judgment and the performance of his duties. By and large his professional weaknesses were observed by Ames' colleagues and supervisors and were tolerated by many who did not consider them highly unusual for Directorate of Operations officers on the "not going anywhere" promotion track. That an officer with these observed vulnerabilities should have been given counter-intelligence responsibilities in Soviet operations where he was in a prime position to learn of the intimate details of the Agency's most sensitive operations, contact Soviet officials openly and then massively betray his trust is difficult to justify. The IG investigative team has been dismayed at this tolerant view of Ames' professional deficiencies and the random indifference given to his assignments, and our recommendations reflect that fact.

Aldrich Hazen Ames

Finally, on the grander scale of how the reaction to the major loss of Soviet cases in 1985-86 was managed, our team has been equally strict, demanding and greatly disturbed by what we saw. If Soviet operations—the effort to achieve human penetrations of the USSR for foreign intelligence and counterintelligence information—was the highest priority mission of the clandestine service of CIA in 1985-86, then the loss of most of our assets in this crucial area of operations should have had a devastating effect on the thinking of the leaders of the DO and CIA. The effort to probe the reasons for these losses should have been of the most vital significance to U.S. intelligence, but particularly to the CIA, and should have been pursued with the utmost vigor and all necessary resources until an explanation—a technical or human penetration—was found.

It is true that the spy was found, but the course to that conclusion could have been much more rapid and direct. While those few who were engaged in the search may have done the best they could with what they had, in this investigation we have concluded that the intelligence losses of 1985-86 were not pursued to the fullest extent of the capabilities of the CIA, which prides itself on being the best intelligence service in the world. The analytical judgments and recommendations in this Report reflect that conclusion. We wish it could have been otherwise.

Frederick P. Hitz
Inspector General

Summary

1. In the spring and summer of 1985, Aldrich H. Ames began his espionage activities on behalf of the Soviet Union. In 1985 and 1986, it became increasingly clear to officials within CIA that the Agency was faced with a major CI problem. A significant number of CIA Soviet sources began to be compromised, recalled to the Soviet Union and, in many cases, executed. A number of these cases were believed to have been exposed by Edward Lee Howard, who fled the United States in September 1985 to avoid prosecution for disclosures he made earlier that year. However, it was evident by fall of 1985 that not all of the compromised sources could be attributed to him.

2. Later in 1985, the first Agency efforts were initiated to ascertain whether the unexplained compromises could be the result of:

a. faulty practices by the sources or the CIA officers who were assigned to handle them (i.e., whether the cases each contained "seeds of their own destruction");

b. a physical or electronic intrusion into the Agency's Moscow Station or Agency communications; or

c. a human penetration within the Agency (a "mole").

Although they were never discounted altogether, the first two theories diminished in favor over the years as possible explanations for the losses. A "molehunt"—an effort to determine whether there was a human penetration, a spy, within CIA's ranks—was pursued more or less continuously and with varying degrees of intensity until Ames was convicted of espionage in 1994, nine years after the compromises began to occur.

3. The 1985-1986 compromises were first discussed in late 1985 with DCI William Casey, who directed that the Deputy Director for Operations (DDO) make every effort to determine the reason for them. In January 1986, SE Division (Soviet East European Division, later renamed Central Eurasia Division, directed operations related to the Soviet Union and its successor states) instituted new and extraordinary compartmentation measures to prevent further compromises. In the fall of 1986, a small Special Task Force (STF) of four officers operating under the direction of the Counter-intelligence Staff (CI Staff) was directed to begin an effort to determine the cause of the compromises. This effort, which was primarily analytic in nature, paralleled a separate FBI task force to determine whether the FBI had been penetrated. The FBI task force ended, and the CIA STF effort diminished significantly in 1988 as its participants became caught up in the creation of the Counterintelligence Center (CIC). Between 1988 and 1990, the CIA molehunt came to a low ebb as the officers involved concentrated on other CI matters that were believed to have higher priority.

4. In late 1989, after his return from Rome, Ames' lifestyle and spending habits had changed as a result of the large amounts of money he had received from the KGB in return for the information he provided. Ames made no special efforts to conceal his newly acquired wealth and, for example, paid cash for a $540,000 home. This unexplained affluence was brought to the attention of the molehunt team by a CIA employee in late 1989, and a CIC officer began a financial inquiry. The preliminary results of the financial inquiry indicated several large cash transactions but were not considered particularly significant at the time.

5. Nevertheless, information regarding Ames' finances was provided to the Office of Security (OS) by CIC in 1990. A background investigation (BI) was conducted and a polygraph examination was scheduled. The BI was very thorough and produced information that indicated further questions about Ames and his spending habits. However, this information was not made available to the polygraph examiners who tested him, and CIC did not take steps to ensure that the examiners would have full knowledge of all it knew about Ames at the time. In April 1991, OS determined that Ames had successfully completed the reinvestigation polygraph with no indications of deception, just as he had five years previously.

6. In 1991, CIA's molehunt was revitalized and rejuvenated. Two counterintelligence officers were assigned full-time to find the cause of the 1985–86 compromises. The FBI provided two officers to work as part of the molehunt team.

7. During this phase, attention was redirected at Ames and a number of other possible suspects. In March 1992, a decision was made to complete the financial inquiry of Ames that had been initiated in 1989. In August 1992, a correlation was made between bank deposits by Ames that were identified by the financial inquiry and meetings between Ames and a Soviet official that the Agency and FBI had authorized in 1985. The joint CIA/FBI analytic effort resulted in a report written in March 1993, which concluded that, among other things, there was a penetration of the CIA. It was expected by CIA and FBI officials that the report, which included lists of CIA employees who had access to the compromised cases, would be reviewed by the FBI in consideration of further investigative steps.

8. The totality of the information available to CIC and the FBI prompted the FBI to launch an intensive CI investigation of Ames. During this phase, the FBI attempted to gather sufficient information to determine whether Ames was in fact engaged in espionage, and the Agency molehunt team was relegated to a supporting role. Every effort was made to avoid alerting Ames to the FBI CI investigation. According to FBI and Agency officials, it was not until a search of Ames' residential trash in September 1993, which produced a copy of an operational note from Ames to the Russians, that they were certain Ames was a spy. After the FBI had gathered additional information, Ames was arrested on February 21, 1994 and pled guilty to espionage on April 28, 1994.

9. The two CIA officers and the two FBI officers who began working in earnest on the possibility of an Agency penetration in 1991 under the auspices of the Agency's CIC deserve credit for the ultimate identification of Ames as a hostile intelligence penetration of CIA. Without their efforts, it is possible that Ames might never have been successfully identified and prosecuted. Although proof of his espionage activities was not obtained until after the FBI began its CI investigation of Ames in 1993, the CIA molehunt team played a critical role in providing a context for the opening of an intensive investigation by the FBI. Moreover, although the CIA and the FBI have had disagreements and difficulties with coordination in other cases in the past, there is ample evidence to support statements by both FBI and CIA senior management that the Ames case was a model of CI cooperation between the two agencies.

Rosario Ames

10. From its beginnings in 1986, however, the management of CIA's molehunt effort was deficient in several respects. These management deficiencies contributed to the delay in identifying Ames as a possible penetration, even though he was a careless spy who was sloppy and inattentive to measures that would conceal his activities. Despite the persistence of the individuals who played a part in the molehunt, it suffered from insufficient senior management attention, a lack of proper resources, and an array of immediate and extended distractions. The existence and toleration of these deficiencies is difficult to understand in light of the seriousness of the 1985-86 compromises and especially when considered in the context of the series of other CI failures that the Agency suffered in the 1980s and the decade-long history of external attention to the weaknesses of the Agency's CI and security programs. The deficiencies reflect a CIA CI function that has not recovered its legitimacy since the excesses of James Angleton, which resulted in his involuntary retirement from CIA in 1974. Furthermore, to some extent, the "Angleton Syndrome" has become a canard that it used to downplay the role of CI in the Agency.

11. Even in this context, it is difficult to understand the repeated failure to focus more attention on Ames earlier when his name continued to come up throughout the investigation. He had access to all the compromised cases; his financial resources improved substantially for unestablished reasons; and his laziness and poor performance were rather widely known. All of these are CI indicators that should have drawn attention to Ames. Combined, they should have made him stand out. Arguably, these indicators played a role in the fact

that Ames was often named as a prime suspect by those involved in the molehunt.

12. One result of management inattention was the failure of CIA to bring a full range of potential resources to bear on this counterespionage investigation. There was an over-emphasis on operational analysis and the qualifications thought necessary to engage in such analysis, and a failure to employ fully such investigative techniques as financial analysis, the polygraph, behavioral analysis interviews, and the review of public and governmental records. These problems were exacerbated by the ambiguous division of the counterespionage function between CIC and OS and the continuing subordination by the Directorate of Operations (DO) of CI concerns to foreign intelligence collection interests. Excessive compartmentation has broadened the gap in communications between CIC and OS, and this problem has not been overcome despite efforts to improve coordination. CIC did not share information fully with OS or properly coordinate the OS investigative process.

13. These defects in the Agency's capability to conduct counterespionage investigations have been accompanied by a degradation of the security function within the Agency due to management policies and resource decisions during the past decade. These management policies emphasize generalization over expertise, quantity over quality, and accommodation rather than professionalism in the security field. This degradation of the security function has manifested itself in the reinvestigation and polygraph programs and appears to have contributed to Ames ability to complete polygraphs successfully in 1986 and 1991 after he began his espionage activities.

14. Beyond defects in counterespionage investigations and related security programs, the Ames case reflects significant deficiencies in the Agency's personnel management policies. No evidence has been found that any Agency manager knowingly and willfully aided Ames in his espionage activities. However, Ames continued to be selected for positions in SE Division, CIC and the Counternarcotics Center that gave him significant access to highly sensitive information despite strong evidence of performance and suitability problems and, in the last few years of his career, substantial suspicion regarding his trustworthiness. A psychological profile of Ames that was prepared as part of this investigation indicates a troubled employee with a significant potential to engage in harmful activities.

15. Although information regarding Ames' professional and personal failings may not have been available in the aggregate to all of his managers or in any complete and official record, little effort was made by those managers who were aware of Ames' poor performance and behavioral problems to identify the problems officially and deal with them. If Agency management had acted more responsibly and responsively as these problems arose, it is possible that the Ames case could have been avoided in that he might not have been placed in a position where he could give away such sensitive source information.

16. The principal deficiency in the Ames case was the failure to ensure that the Agency employed its best efforts and adequate resources in determining on a timely basis the cause, including the possibility of a human penetration, of the compromises in 1985–86 of essentially its entire cadre of Soviet sources. The individual officers who deserve recognition for their roles in the eventual identification of Ames were forced to overcome what appears to have been significant inattentiveness on the part of senior Agency management. As time wore on and other priorities intervened, the 1985–86 compromises received less and less senior management attention. The compromises were not addressed resolutely until the spring of 1991 when it was decided that a concerted effort was required to resolve them. Even then, it took nearly three years to identify and arrest Ames, not because he was careful and crafty, but because the Agency effort was inadequate.

17. Senior Agency management, including several DDOs, DO Division Chiefs, CIC and DO officials, should be held accountable for permitting an officer with obvious problems such as Ames to continue to be placed in sensitive positions where he was able to engage in activities that have caused great harm to the United States. Senior Agency management, including at least several DCIs, Deputy Directors, DO Division Chiefs, and senior CI and security officials, should also be held accountable for not ensuring that the Agency made a maximum effort to resolve the compromises quickly

through the conduct of a focused investigation conducted by adequate numbers of qualified personnel.

What was Ames' Career History with CIA?

18. In June 1962, Ames completed full processing for staff employment with the Agency and entered on duty as a GS-4 document analyst in the Records Integration Division (RID) of the DO. Within RID, Ames read, coded, filed, and retrieved documents related to clandestine operations against an East European target. He remained in this position for five years while attending George Washington University, on a part-time or full-time basis. In September 1967, Ames received his Bachelor of Arts degree in history with an average grade of B-.

19. Ames originally viewed his work with RID as a stopgap measure to finance his way through college. However, he grew increasingly fascinated by intelligence operations against Communist countries, and, influenced by other RID colleagues who were entering the Career Trainee (CT) program, he applied and was accepted as a CT in December 1967. When Ames completed this training nearly a year later, he was assigned to an SE Division branch. He remained there for several months before beginning Turkish language studies.

20. Ames' first overseas posting took place between 1969 and 1972. It was not a successful tour, and the last Performance Appraisal Report (PAR) of his tour stated, in effect, that Ames was unsuited for field work and should spend the remainder of his career at Headquarters. The PAR noted that Ames preferred "assignments that do not involve face-to-face situations with relatively unknown personalities who must be manipulated." Such a comment was devastating for an operations officer, and Ames was discouraged enough to consider leaving the Agency.

21. Ames spent the next four years, 1972-76, at Headquarters in SE Division. Managing the paperwork and planning associated with field operations at a distance was more comfortable for Ames than trying to recruit in the field himself, and he won generally enthusiastic reviews from his supervisors. One payoff from this improved performance was the decision in September 1974 to name Ames as both the Headquarters and field case officer to manage a highly valued Agency asset.

22. Ames' opportunity to expand his field experience came with his assignment to the New York Base of the DO's Foreign Resources Division from 1976 to 1981. The PARs that Ames received during the last four of his five years in New York were the strongest of his career. These PARs led Ames to be ranked in the top 10% of GS-13 DO operations officers ranked for promotion in early 1982. He was promoted to GS-14 in May 1982.

23. The career momentum Ames established in New York was not maintained during his 1981-83 tour in Mexico City. This assignment, like his earlier tour and his later tour in Rome, failed to play to Ames' strengths as a handler of established sources and emphasized instead an area where he was weak—the development and recruitment of new assets. In Mexico City, Ames spent little time working outside the Embassy, developed few assets, and was chronically late with his financial accountings. Further, Ames developed problems with alcohol abuse that worsened to the point that he often was able to accomplish little work after long, liquid lunches. His PARs focused heavily, and negatively, on his failure to maintain proper accountings and were generally unenthusiastic. In Mexico City, Ames also became involved in an intimate relationship with the Colombian cultural attache, Maria del Rosario Casas Dupuy.

24. Despite his lackluster performance in Mexico City, Ames returned to Headquarters in 1983 to a position that he valued highly. His appointment as Chief of a branch in an SE Division Group was recommended by the officer who had supervised Ames in New York and approved by Chief, SE Division and the DDO. This position gave him access to the Agency's worldwide Soviet operations. Ames completed this tour with SE Division by being selected by the SE Division Chief as one of the primary debriefers for the defector Vitaly Yurchenko from August to September 1985. For his work in the SE Division Group, Ames was ranked very near the lower quarter of DO operations officers at his grade at this time.

25. By early 1984, Ames was thinking ahead to his next field assignment and asked to go to Rome as Chief of a branch where he had access to information regarding many operations run or supported from that post. He left for Rome in 1986. He once again began to drink

heavily, particularly at lunch, did little work, sometimes slept at his desk in the afternoons, rarely initiated developmental activity, and often fell behind in accountings, reporting and other administrative matters. Ames was successful in managing liaison relations with U.S. military intelligence units in Italy, but he registered few other achievements.

26. Ames' mediocre performance for the Agency in Rome did not prevent his assignment upon his return to Headquarters in mid-1989 to head a branch of an SE Division Group. Here again he had access to many sensitive cases. When that position was eliminated in a December 1989 reorganization of SE Division, Ames became Chief of another SE Division branch, where he remained until late 1990. At this time, Ames was ranked in the bottom 10% of DO GS-14 operations officers. He appears to have been a weak manager who focused only on what interested him.

27. Ames moved to a position in the Counter-intelligence Center in October 1990. In the CIC, where he remained until August 1991, he prepared analytical papers on issues relating to the KGB but also had access to sensitive data bases. Discussions between Ames and the Deputy Chief, SE Division, resulted in Ames temporary return to SE Division as head of a small KGB Working Group between August and November 1991.

28. In 1991, Chief SE Division requested that a counternarcotics program be established through liaison with the states of the former Soviet Union. Thereafter, Ames began a rotation to the Countenarcotics Center (CNC) in December 1991. At CNC, where Ames remained until his arrest, he worked primarily on developing a program for intelligence sharing between the United States and cooperating countries.

29. Ames was arrested on February 21, 1994. On that date, DCI Woolsey terminated his employment with the Agency.

What were Ames' Strengths, Weaknesses and Vulnerabilities?

Performance Problems

30. Ames appears to have been most successful and productive in assignments that drew on his:

Analytical skills, particularly collating myriad bits of information into coherent patterns;

Writing skills, both in drafting operational cables and crafting more intuitive thought pieces;

Intellectual curiosity and willingness to educate himself on issues that were beyond the scope of his immediate assignment; and

Creativity in conceiving and implementing sometimes complex operational schemes and liaison programs.

31. Ames was far less successful—and indeed was generally judged a failure—in overseas assignments where the development and recruitment of assets was the key measure of his performance. For most of his career, moreover, a number of work habits also had a dampening impact on his performance. These included:

Inattention to personal hygiene and a sometimes overbearing manner that aggravated the perception that he was a poor performer;

A lack of enthusiasm for handling routine administrative matters. By the late 1970's, when Ames was assigned to New York, this pattern of behavior was evident in his tardy filing of financial accountings and failure to document all of his meetings in contact reports. Ames' disdain for detail also manifested itself in his pack-rat amassing of paper and his failure, especially in Rome, to handle action cables appropriately and expeditiously; and

Selective enthusiasm. With the passage of time, Ames increasingly demonstrated zeal only for those few tasks that captured his imagination while ignoring elements of his job that were of little personal interest to him.

Sleeping on the Job

32. A significant number of individuals who have worked with Ames in both domestic and foreign assignments state that it was not uncommon for Ames to be seen asleep at his desk during working hours. This behavior often coincided, especially in Rome and at

Headquarters in the 1990's, with Ames having returned from lunch where he consumed alcohol.

Failure to File Required Reports

33. The Agency has an established system of reports of various kinds that serve administrative, operational, security, and counterintelligence purposes. Ames paid very little attention to a variety of these reporting requirements. His attention to these matters was by and large ignored, to the extent it was known by Agency management.

Foreign Travel

34. Over the course of several years, Ames failed to report foreign travel to OS as required by Headquarters Regulation. It is difficult to determine whether and to what extent management was aware of his unreported travel. The official record includes no mention, but fellow employees appear to have had some knowledge of his travels, especially in Rome.

Contact Reports

35. Ames also failed to file timely contact reports regarding many of his meetings with foreign officials. While this failure originally may have been related to his laziness and disdain for regulations, it became more calculated and had serious CI implications once he had volunteered to the Soviets in 1985. Ames states that he deliberately avoided filing complete and timely reports of his contacts with Soviet officials in Washington. If he had done so, he believes, Agency and FBI officials might have identified contradictions. Moreover, he believes they would have seen no operational advantage to the meetings, ceased the operation, and removed the ready pretext for his espionage activities. This also was true of his meetings with Soviets in Rome.

Financial Accountings

36. Throughout the course of Ames' career, managers reported that they frequently counseled and reprimanded him, or cited in his PAR Ames' refusal to provide timely accountings and properly maintain his revolving operational funds. This is more than a question of financial responsibility for DO officers. It also provides DO managers with another means of monitoring and verifying the activities of the operations officers they supervise.

Foreign National Contacts and Marriage

37. Ames also did not fully comply with Agency requirements in documenting his relationship with Rosario. He never reported his intimate relationship with her as a "close and continuing" one while he was in Mexico City. Management was aware generally of a relationship but not its intimate nature and did not pursue the reporting. He did follow proper procedures in

L to R: NACIC officers Rusty Capes and Anna Kline; FBI Special Agent Les Wiser; who was in charge of the Ames Investigation and NACIC Branch Chief Frank Rafalko.

obtaining approval for their marriage. However, Agency management did not accept or implement properly the CI Staff Chief's recommendation at the time that Ames be placed in less sensitive positions until Rosario became a U.S. citizen.

Security Problems

38. Ames also seemed predisposed to ignore and violate Agency security rules and regulations. In New York in 1976, he committed a potentially very serious security violation when he left a briefcase full of classified information on a New York subway train. In 1984, Ames brought Rosario to an Agency-provided apartment; a clear violation that compromised the cover of other operational officers. Ames also committed a breach of security by leaving a sensitive secure communications system unsecured at the FR/New York office. On July 2, 1985, Ames received the only official security violation that was issued to him when he left his office safe open and unlocked upon departure for the evening. Ames admits to using his home computer occasionally when in Rome between 1986 and 1989 to draft classified memoranda and cables that he would print out and take into the office the next day. In the most extreme example of his disregard for physical security regulations, of course, Ames wrapped up five to seven pounds of cable traffic in plastic bags in June 1985 and carried it out of Headquarters to deliver to the KGB.

Alcohol Abuse

39. Much has been made since his arrest of Ames' drinking habits. While it is clear that he drank too much too often and there is some basis to believe this may have clouded his judgment over time, he does not appear to have been an acute alcoholic who was constantly inebriated. Ames acknowledges the presence of a variety of symptoms of alcohol addition. The term "alcoholic" often conjures up images of broken individuals who spend their days helplessly craving a drink, becoming intoxicated beyond any self-control, and only breaking out of their intoxication with severe withdrawal symptoms. As explained in the psychological profile prepared by the psychologist detailed to the IG, alcohol addiction is, in reality, a more subtle, insidious process. This accounts for the fact that many of Ames' colleagues and a few supervisors were able to work with Ames without noticing his substance abuse problem.

40. In regard to why they did not deal with problems associated with Ames' alcohol abuse, several Agency managers say that alcohol abuse was not uncommon in the DO during the mid–to late–1980's and that Ames' drinking did not stand out since there were employees with much more serious alcohol cases. Other managers cite a lack of support from Headquarters in dealing with problem employees abroad.

41. Medical experts believe that alcohol, because it diminishes judgment, inhibitions, and long-term thinking ability, may play some role in the decision to commit espionage. At the same time, because the number of spies is so small relative to the fraction of the U.S. population that has an alcohol abuse problem, statistical correlation cannot be made. As a result, alcohol abuse cannot be said to have a predictive connection to espionage and, in and of itself, cannot be used as an indicator of any real CI significance.

Financial Problems

42. In 1983-85, Ames became exceedingly vulnerable to potential espionage as a result of his perception that he was facing severe financial problems. According to Ames, once Rosario moved in with him in December 1983 he had begun to feel a financial pinch. Ames describes being faced with a credit squeeze that included a new car loan, a signature loan that had been "tapped to the max," mounting credit card payments, and, finally, a divorce settlement that he believed threatened to bankrupt him.

43. Ames claims to have first contemplated espionage between December 1984 and February 1985 as a way out of his mounting financial dilemma. Confronting a divorce that he knew by that time was going to be financially draining, and facing added expenses connected with his imminent marriage to someone with already established extravagant spending habits, Ames claims that his financial predicament caused him to commit espionage for financial relief.

Why did Ames Commit Espionage?

44. Ames states that his primary motivating factor for his decision to commit espionage was his desperation regarding financial indebtedness he incurred at the time of his separation from his first wife, their divorce settlement and his cohabitation with Rosario. He also

says that several otherwise inhibiting "barriers" had been lowered by:

a. the opportunity to meet Soviet officials under Agency sanction;

b. the lack of concern that he would soon be subject to a reinvestigation polygraph;

c. his fading respect for the value of his Agency work as a result of lengthy discussions with Soviet officials; and

d. his belief that the rules that governed others did not apply to him.

Ames claims he conceived of a one-time "scam" directed against the Soviets to obtain the $50,000 he believed he needed to satisfy his outstanding debt in return for information about Agency operations he believed were actually controlled by the Soviets. He recognized subsequently that there was no turning back and acted to protect himself from the Soviet intelligence services by compromising Agency sources first in the June 1985 "big dump."

How were Indications of Substantial Changes in Ames Financial Situation Handled?

45. The financial inquiry regarding Ames began in November 1989 with the receipt of information from at least one Agency employee that Ames' financial situation had changed and he was living rather extravagantly. Upon his return from Rome, Ames purchased a home in Arlington for more than a half million dollars in cash and made plans to remodel the kitchen and landscape the yard, sparing no expense. Ames was also known to have purchased a Jaguar automobile and to have Filipino servants whom he had flown to and from the Philippines. Ames' lifestyle change was apparent to others as well as several employees state that they noticed at that time a marked improvement in Ames' physical appearance, including capped teeth and expensive Italian suits and shoes.

46. The financial inquiry faltered over resource limitations and priority conflicts, was reinvigorated in March 1992 and was not completed until mid-1993. The information obtained as a result of the Ames financial review, especially the correlation between deposits made by the Ameses and the operational meetings, was an essential element in shifting the focus of the molehunt toward Ames and paving the way, both psychologically and factually, for the further investigation that resulted in his arrest. Yet the financial review was permitted to stall for almost a year while other matters consumed the time and effort of the single CIC officer who possessed the interest and ability to necessary to conduct it. Technical management expertise to oversee the investigator's activities and help guide him was lacking. Given the responsibility that was placed on the investigator and his relative inexperience in conducting and analyzing financial information, he did a remarkable job. But there was clearly a lack of adequate resources and expertise available in CIC for this purpose.

47. If the financial inquiry had been pursued more rapidly and without interruption, significant information about Ames' finances would have been acquired earlier.

Was the Counterespionage Investigation Coordinated Properly with the FBI?

48. Under Executive Order 12333, CIA is authorized to conduct counterintelligence activities abroad and to coordinate the counterintelligence activities of other agencies abroad. The Order also authorizes CIA to conduct counterintelligence activities in the United States, provided these activities are coordinated with the FBI. Under a 1988 CIA-FBI Memorandum of Understanding (MOU) the FBI must be notified immediately when there is a reasonable belief that an individual may engage in activities harmful to the national security of the United States.

49. CIA-FBI cooperation in the Ames case after the spring of 1991 generally exceeded the coordination requirements under the 1988 MOU. The FBI could have taken over the Ames case completely in 1991 but apparently concluded that it did not have sufficient cause to open an intensive CI investigation directed specifically at Ames. The FBI officers who were part of the team were provided unprecedented access to CIA information related to Ames and to other CIA cases. These FBI officers indicate that they had full access to all of the CIA information they needed and requested. Once the FBI did take over the case in 1993, CIA cooperation with the Bureau was excellent, according to FBI and CIA accounts.

Were Sufficient Resources and Management Attention Devoted to the Ames Investigation?

50. In consideration whether the resources that were applied to the molehunt were sufficient, it is necessary to evaluate the need for secrecy and compartmentation. If alerting a potential mole to the investigation was to be avoided at all costs, then concerns about the size and discretion if any group undertaking the investigation would be paramount. Nevertheless there must be some balance between secrecy and progress. Despite the arguments for the small size of the molehunt team, many officers concede that more resources could have been brought to bear earlier on the Ames investigation.

51. Even accepting the argument that the team had to be small to maintain compartmentation and to manage a complex CI investigative process, the resource issue remains because the molehunt team members who were made available were not focused exclusively on the task, but were frequently diverted to other requirements. The limited size and diffused focus of the molehunt team does not support DO management's assertions that the 1985-86 compromised Soviet cases were "the biggest failure a spy Agency could have." Rather, the resources applied to the task force indicate lack of management attention to this most serious of intelligence failures.

52. The resources that the Agency devoted to the molehunt were inadequate from the outset, especially when considered in light of the fact that the 1985-86 compromises were the worst intelligence losses in CIA history.

Has Agency Use of Polygraphs and Background Investigations been Sufficient to Detect Possible Agency Counterintelligence Problems at the Earliest Time?

53. The fact that Ames conceived, executed and sustained an espionage enterprise for almost nine years makes it difficult to argue that Agency screening techniques functioned adequately to detect a CI problem at the earliest possible time. The question then becomes whether the screening techniques, particular the periodic polygraph examination, were adequate and why they did not detect Ames. The available evidence indicates that there were weaknesses in the polygraph methods that were used. However, it is difficult to conclude that the techniques themselves are inadequate since the major failing in the Ames case appears to be traceable to non-coordination and non-sharing of derogatory information concerning Ames.

54. Although this IG investigation necessarily focused on the Ames polygraph and background investigations, many employees of the Office of Security also raised generic problems in these programs. At a minimum, these expressions of concern about the Agency's polygraph program reflect a significant morale problem.

55. In light of the dominant role that the polygraph plays in the reinvestigation process, OS management came to be interested in production. For most of the time since 1986—when the five-year periodic reinvesti-

Ames arrest at his car.

gation program was begun—until the present, the reinvestigation program has been behind schedule. As a result, OS managers have stressed the successful completion of polygraph examinations. Many examiners believe that this requirement implicitly stressed quantity over quality. In addition to the pressures of production, the lack of experience in the polygraph corps has detrimentally affected the Agency's polygraph program. The 1988 IG inspection of the polygraph program noted this loss of experience. Many current and former OS polygraphers say that the OS policy of promoting generalists has caused the loss of experience. Many individuals also cite the lack of complete information on testing subjects as a defect in the Agency's polygraph program.

56. The 1986 polygraph of Ames was deficient and the 1991 polygraph sessions were not properly coordinated by CIC after they were requested. The Office of Security (OS) conducted a background investigation (BI) prior to Ames' polygraph examination in 1991. This 1991 BI is deemed by OS personnel to be a very professional and in-depth investigation of Ames' personal and professional activities. The investigator who conducted this BI deserves great credit for the competency and thoroughness of her efforts. Unfortunately, the results of this 1991 BI were not available to the polygraph examiners at the time they tested Ames nor was financial information that had been developed by CIC. Ultimately, the miscommunication between CIC and OS components that were involved led the individual examiners to conduct standard reinvestigation polygraph tests that Ames passed. Both examiners say that having such detailed information available could have significantly altered their approach to testing Ames.

To what Extent did Ames Use Computer Access and Capabilities to Engage in Espionage Activities?

57. Ames reports that he bought his first computer in the late winter or early spring of 1986 just prior to leaving for Rome. Ames' interest, however, was limited to computer applications rather than the technical aspects of computer science or programming. Ames admits to using his home computer occasionally when in Rome to draft classified memoranda and cables that he would print out and take into the office the next day. Ames admits to writing all his notes to the Soviets on his home computer using WordPerfect word processing software while in Rome. These notes, however, were passed only in paper form. Ames began preparing at home and passing computer disks to the Soviets after returning to Washington. These disks had been password-protected by the Russians. The information contained on the disks, according to Ames, consisted only of one or two-page messages from him to his handler. All other information he passed was in the form of paper copies of documents. The intent was for Ames to leave a disk at a drop site and have the same disk returned later at his pick-up site.

58. Ames says that passing disks and using passwords was entirely his idea. Although Ames admits to discussing Agency computer systems with the Soviets, he says it was obvious that his handlers had little or no expertise in basic computer skills. Ames describes his handlers as being "rather proud of their having been able to turn a machine on, crank up WordPerfect and get my message on it."

59. Ames states consistently that he did not use or abuse computer access as a means for enhancing his espionage capabilities. He explains that the computer systems to which he had access in CIC, SE/CE Division and Rome Station were "really no more than bona fide electric typewriters." He does say, however, that this changed after he was given access to the CNC Local Area Network (LAN). That LAN featured the DO's message delivery system (MDS). However, the CNC terminals differed from DO LANs in that the capability to download information to floppy disks had not been disabled in the CNC LAN. The combination of having the MDS system available on terminals that had floppy disk capabilities represented a serious system vulnerability.

60. Ames clearly viewed his access to the CNC LAN as a very significant event in his ability to conduct espionage. The broadened access, combined with the compactness of disks, greatly enhanced the volume of data he could carry out of Agency facilities with significant reduced risk. Fortunately, he was arrested before he could take full advantage of this system vulnerability.

61. No specific precautions were taken by Agency officials to minimize Ames' computer access to information within the scope of his official duties. In

fact, there is one instance where Ames was granted expanded computer access despite expressions of concern by CIC and SE Divison management at the time about his trustworthiness. Ames states he was surprised when he signed on and found that he had access to information about double agent cases. This allowed him to compromise a significant amount of sensitive data from the CIC to which he did not have an established need-to-know.

Is There any Merit to the Allegations in the "Poison Fax?"

62. In April 1994, an anonymous memorandum was faxed to the Senate Select Committee on Intelligence criticizing CIA counterintelligence policies and practices. That memorandum, which came to be known as the "poison fax," also alleged that an SE Division manager had warned Ames he was suspected of being a KGB mole and that a message from the field confirmed this. These allegations were featured in the press and raised questions in the Congress. No evidence has been found to substantiate these allegations.

Has CIA Been Effectively Organized to Detect Penetrations Such as Ames?

63. During the period of the Agency molehunt that led to Ames, the CI function and its counterespionage element was divided between the DO and OS. This division created problems that adversely affected the Agency's ability to focus on Ames. Although attempts were made to overcome these problems by written understandings and the assignment of OS officers to CIC, these attempts were not altogether successful.

64. Senior security officials have pointed out that there always has been a "fault line" in communications between the CIC, and its predecessors, and the OS. This division has created a number of problems, given the disparate cultures of the two organizations. Attempts are being made to employ CIC-OS teams to overcome these problems, but the problems are inherent to the division of CI responsibility for CI between CIC and OS interfered with a comprehensive approach to the molehunt. When financial leads were obtained in 1989 and 1990, CIC essentially turned the matter over to OS for Ames' investigation but failed to communicate all the relevant facts effectively with the OS personnel who were involved in the reinvestigation.

65. Many senior managers and other officers have strong opinions regarding whether the Agency's CI element, at least the portion that handles possible penetrations of the Agency, should report through the DDO. A number of officers believe that taking the CI function out of the DO would permit the addition of personnel who are not subject to the limitations of the DO culture and mindset. Other officers view the prospect of taking counterespionage outside the DO as impossible and potentially disastrous. Doing so, they argue, would never work because access to DO information would become more difficult. Some officers also argue that reporting directly to the DCI would be copying the KGB approach, which proved over the years to be unworkable. As a counter argument, however, former DCI Webster believes, in retrospect, that the CIC he created in 1988 should have reported to him directly with an informational reporting role to the DDO.

Were CIA Counterintelligence Personnel Who Conducted the Molehunt Properly Qualified by Training and Experience?

66. Of the four officers who were assigned to the STF in 1986, one remained when the molehunt team was established in CIC in 1991 to continue to pursue the cause of the 1985-86 compromises. That officer was chosen to head the effort primarily because she was an experienced SE Division officer, was familiar with the KGB and wanted to pursue the compromises. According to her supervisor, there were not many other employees who had the years of experience, the operational knowledge, the interest, the temperament, and the personality to persist in this effort. She was joined by another officer who had headed the Moscow Task Force inquiry charged with doing the DO damage assessment concerning the Lonetree/Bracy allegations. A third officer, who had been on rotation to CIC from the Office of Security was chosen to assist the team because of his background and CI experience, although he was not actually made a team member until June 1993. While this investigator was certainly not the only person in CIA who was capable of performing a financial analysis, he was the only one who was known to, and trusted by, the team leader. He was ideal in her view because of his previous work with her on other CI cases. In addition, two FBI officers were assigned to the effort.

67. Put most simply, the consensus view of those in CIC who were directly involved in the molehunt seems to be that good CI officers have both innate and learned characteristics that make them effective. In addition to innate CI ability, a good CI analyst needs a great deal of general and particular knowledge to make the mental connections necessary to conduct a CI investigation. General knowledge in the molehunt context refers to knowledge of the KGB, while particular knowledge refers to knowledge of the 1985-86 compromised cases. In addition, many CIC employees say that operational experience is essential to CI work. Although this general and particular knowledge can be acquired through study, for the most part it is obtained over years of experience actually working on foreign intelligence operations and CI cases in a particular subject area.

68. In the judgment of the IG, these criteria for qualifications as a CI analyst and for the process of conducting a CI investigation reflect a very narrow view of the scope and nature of CI investigations. In the Ames case, it was unduly cramped and justified an unfortunate resistance to adding more personnel to the molehunt unless they were deemed by the team leader to be qualified. Further, this view of counterespionage presents significant risks both to the Agency and successful prosecutions in the future. In the Ames investigation, the equities of any future prosecution were protected by the fact of FBI participation. Law enforcement officers bring an understanding of investigative procedure critical to building a successful prosecution. Without FBI participation, the risk of the narrow CIC view is that prosecutions may be jeopardized in future CI investigations. In addition to protecting Agency and prosecutive equities, training in law enforcement and other investigative techniques would expand the scope of information and techniques available to the Agency's CI investigators.

69. Despite these general shortcomings in CI training and methodology, the molehunters performed admirably. Their work included useful analysis that helped advance the resolution of the 1986-86 compromises significantly. On occasion, their work also went beyond the scope of what had been considered an adequate CI investigation to that point. Thus, they advanced the art form of CI investigations within the CIA. In the final analysis, they contributed substantially to catching a spy.

Was the Molehunt that led to Ames Managed Properly, and Who was Responsible?

70. Supervisors responsibility for the molehunt that eventually led to Ames shifted over time as managers, organizations and circumstances changed.

71. The primary responsibility for the molehunt within the Agency rested with officials in the CI Staff, later the CIC, as well as senior DO management. Management of the molehunt during the initial, analytic phase was inconsistent and sporadic. Although keen interest was expressed from time to time in determining what went wrong, the resources devoted to the molehunt were quite modest, especially considering the significance to the DO and the Agency of the rapid compromise of essentially all major Soviet sources. Those directly engaged in the molehunt also had to contend with competing assignments and were distracted from the molehunt by other possible explanations for the compromises, such as technical penetrations and the Lonetree/Bracy case, that eventually proved not to be fruitful. Senior CI managers at the time admit that they could, and probably should, have devoted more resources to the effort.

72. In the CI staff, the early years of the molehunt were primarily analytical and episodic, rather than investigative and comprehensive. Although information gathering and file review are important, little else appears to have been done during this time. A number of CI cases concerning Agency employees were opened based on suspicious activity, but none were brought to resolution. No comprehensive list of Agency officers with the requisite access was created and analyzed during this stage in an attempt to narrow the focus of the molehunt.

73. SE Division management must also assume some responsibility, given the fact that the 1985-86 compromises involved major SE Division assets. SE Division management should have insisted upon an extensive effort and added its own resources if necessary to determine the cause of the compromises. It is not sufficient to say, as these and many other officials now do, that they did not more closely monitor or encourage the molehunt effort because they knew they were suspects themselves and did not wish to appear to be attempting to influence the matter in an undue fashion. The distinction between encouraging a responsible effort

and improperly interfering in the process of that effort is considerable. In any event, another senior SE official who was not on the list could have been given the necessary authority and responsibility.

74. Given the importance of the compromises and the need to determine their cause, the DDOs during this phase also must bear responsibility for not paying more attention to and better managing the molehunt.

75. Beyond those in the DO and CIC who had direct responsibility for the molehunt during this phase, OS should have done a better job of developing leads that would have assisted the molehunt team in focusing its attention on Ames as early as 1986. In the mid-1980s, OS had fallen behind in its reinvestigation polygraphs, and many officers had not been repolygraphed for periods much longer than the required five-year intervals. Ames had not been polygraphed for almost ten years when he was scheduled for a reinvestigation polygraph in 1986. That polygraph raised several questions but failed to reveal any problems despite the fact he had begun spying for the Soviets a year earlier and he reports he was very apprehensive at the time about being exposed.

76. The reorganization of OS in 1986 was followed in 1988 by the creation of the CIC which included a large OS contingent as an integral part of the CIC. While one of the purposes of CIC was to consolidate all of the Agency's CI resources in a single component, the result was an overlap of missions, jurisdictional struggles at the highest levels of OS and CIC, and a failure to share information. According to a May 1991 Office of Inspector General Report of Inspection concerning OS, these problems were caused by the failure of Agency management to define the relative responsibilities of the two components, to provide a mechanism for a smooth flow of information between them, and to establish policy for managing cases of common interest.

77. CIC and the FBI can be credited for initiating a collaborative effort to revitalize the molehunt in April 1991. However, CIC management must also bear responsibility for not allocating sufficient dedicated resources to ensure that the effort was carried out thoroughly, professionally and expeditiously. The delay in the financial inquiry can be attributed largely to the lack of investigative resources allocated to the effort. The CIC investigator deserves a great deal of credit for his initiative and interest in financial analysis and it appears clear that an inquiry into Ames finances would not have occurred to anyone else in CIC had he not been available to suggest it and carry it out. However, the failure to either dedicate the investigator fully to this inquiry before 1992, or to bring in other officers who would have been able to conduct a similar or more thorough financial analysis of Ames, represents one of the most glaring shortcomings of the molehunt. This failure alone appears to have delayed the identification of Ames by at least two years.

78. In 1993, when the FBI opened an intensive CI investigation of Ames, the Agency was fully cooperative and provided excellent support to the FBI's investigation. CIA deferred to the FBI decisions regarding the investigation and allowed Ames continued access to classified information in order to avoid alerting him and to assist in developing evidence of his espionage. The common goal was to apprehend Ames, while safeguarding evidence for a successful prosecution. As has been stated earlier, the CIA/FBI working relationship during the FBI phases appears to have been a model of cooperation.

The White House

Office of the Press Secretary

For Immediate Release *May 3, 1994*

Statement By The Press Secretary

U.S. Counterintelligence Effectiveness

President Clinton signed today a Presidential Decision Directive on U.S. counterintelligence effectiveness to foster increased cooperation, coordination and accountability among all U.S. counterintelligence agencies. The President has directed the creation of a new national counterintelligence policy structure under the auspices of the National Security Council. In addition, he has directed the creation of a new National Counterintelligence Center, initially to be led by a senior executive of the Federal Bureau of Investigation. Finally, the President's Decision Directive requires that exchange of senior managers between the CIA and the FBI to ensure timely and close coordination between the intelligence and law enforcement communities.

The President's decision to take these significant steps of restructuring U.S. counterintelligence policy and interagency coordination, followed a Presidential Review of U.S. counterintelligence in the wake of the Aldrich Ames espionage investigation. The President, in issuing this Directive, has taken immediate steps to improve our ability to counter both traditional and new threats to our nation's security in the post-Cold War era.

Fact Sheet:
U.S. Counterintelligence Effectiveness

Many threats to the national security of the United States have been significantly reduced by the break-up of the Soviet Union and the end of the Cold War. Core U.S. concepts—democracy and market economics—are more broadly accepted around the world than ever before. Nevertheless, recent events at home and abroad make clear that numerous threats to our national interests — terrorism, proliferating weapons of mass destruction, ethnic conflicts, sluggish economic growth— continue to exist and must be effectively addressed. In this context, it is critical that the U.S. maintain a highly effective and coordinated counterintelligence capability.

A review of U.S. counterintelligence effectiveness in the wake of the Ames case highlights the need for improvements in the coordination of our counterintelligence (CI) activities. The recent DCI and Attorney General Joint Task Force on Intelligence Community-Law Enforcement Relations noted that changes to the basic underlying legal authorities defining the relationship between the intelligence and law enforcement communities are not required. Rather, the task force concluded that what is needed..." is for the two communities to improve their understanding of their respective needs and operating practices...to cooperate earlier, more closely, and more consistently on matters in which they both have a separate but parallel interest." This Directive outlines specific steps which will be taken to achieve the objective of improved cooperation.

Keith Hall, first Chairman of National Counterintelligence Board.

Executive Order 12333 designates the National Security Council (NSC) "as the highest Executive Branch entity that provides review of, guidance for and direction to the conduct of," among other things, counterintelligence policies and programs. Consistent with E.O. 12333, the President directed the creation of a new CI structure, under the direction of the NSC, for the coordination of CI policy matters in order to integrate more fully government-wide counterintelligence capabilities, to foster greater cooperation among the various departments and agencies with CI responsibilities and to establish greater accountability for the creation of CI policy and its execution. This new structure will ensure that all relevant departments and agencies have a full and free exchange of information necessary to achieve maximum effectiveness of the U.S. counterintelligence effort, consistent with U.S. law.

Nothing in this directive amends or changes the authorities and responsibilities of the DCI, Secretary of Defense, Secretary of State, Attorney General or Director of the FBI, as contained in the National Security Act of 1947, other existing laws and E.O. 12333.

The following specific initiatives will be undertaken to improve U.S. counterintelligence effectiveness:

National Counterintelligence Policy Coordination

A National Counterintelligence Policy Board (Policy Board) is hereby established and directed to report to the President through the Assistant to the President for National Security Affairs. The existing CI policy and

coordination structure, the National Advisory Group for Counterintelligence, is hereby abolished and its CI functions transferred to the Policy Board.

The Policy Board will consist of one senior executive representative each from DCI/CIA; the FBI; the Departments of Defense, State, and Justice; a Military Department CI component; and the NSC, Special Assistant to the President and Senior Director for Intelligence Programs.

The Chairman of the Policy Board will be designated by the DCI in consultation with the Assistant to the President for National Security Affairs. The Chairman will serve for a period of two years. The position of Chairman of the Policy Board will be rotated among the CIA, FBI, and Department of Defense.

The Policy Board will consider, develop and recommend for implementation to the Assistant to the President for National Security Affairs policy and planning directives for U.S. counterintelligence. The Policy Board will be the principal mechanism for reviewing and proposing to the NSC staff legislative initiatives and executive orders pertaining to U.S. counterintelligence. This Board will coordinate the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements.

A National Counterintelligence Operations Board (Operations Board) will be established under the Policy Board with senior CI representatives from CIA, FBI, DoD, the Military Department CI components, NSA, State, Justice, and Chief of the National CI Center established below.

The Chairman of the Operations Board will be appointed by the Policy Board from among the CIA, FBI, or DoD, and rotated every two years. The Chairmanship of the Policy Board and the Operations Board will not be held by the same agency at any one time. The Operations Board will discuss and develop from an operational perspective matters to be considered or already under consideration by the Policy Board. It will oversee all coordinating subgroups, resolve specific conflicts concerning CI operations and investigations and identify potential CI policy conflicts for referral to the Policy Board.

Counterintelligence Integration and Cooperation

The Policy Board, with the assistance of the DCI and the cooperation of the Director of the FBI, the Secretary of Defense, and the Secretary of State, will establish a National Counterintelligence Center within 90 days of this directive.

A senior FBI executive with CI operational and management experience will serve as the Chief of the National CI Center and a senior Military Department CI component executive will serve as the Deputy Chief of the National CI Center. These agencies will hold these positions for an initial period of 4 years, after which, with the approval of the National CI Policy Board and in consultation with the Assistant to the President for National Security Affairs, the leadership positions will rotate, for 2 year terms, among the FBI, DoD and CIA. At all such times that the FBI does not hold the position of Chief, it will hold the position of Deputy Chief.

The National Counterintelligence Center will be located, staffed and initially structured as recommended in PDD-44.

The National Counterintelligence Center will implement interagency CI activities as described in PDD-44 and report to the Policy Board.

The National Counterintelligence Center will serve as the interagency forum for complementary activities among CI agencies. The CIA's Counterintelligence Center will serve as the CI component for the CIA and execute on behalf of the DCI his authorities to coordinate all U.S. counterintelligence activities overseas.

The Chief of the CIA's Counterintelligence Center Counterespionage Group will be permanently staffed by a senior executive from the FBI.

CIA counterintelligence officers will permanently staff appropriate management positions in the FBI's National Security Division and/or FBI Field Offices.

The Policy Board will be responsible for the regular monitoring and review of the integration and coordination of U.S. counterintelligence programs. The Policy Board will provide an annual report to the Assistant to the President for National Security Affairs on U.S. counterintelligence effectiveness.

Preparing for the 21st Century: An Appraisal of U.S. Intelligence

Background

On 1 March 1996, the Commission on the Roles and Capabilities of the United States Intelligence Community—generally known as the Aspin-Brown Commission—released its final report entitled *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. This Commission was chartered by Congress in October 1994 to conduct a comprehensive review of American intelligence. The Commission began operation on 1 March 1995 and conducted a rigorous inquiry during the following year. A distinguished panel of 17 individuals composed the Commission, which was first chaired by Les Aspin until his untimely death on 21 May 1995 and then by Dr. Harold Brown. It reviewed 19 separate issues that were identified by Congress for assessment. The Commission received formal testimony from 84 witnesses, and its staff interviewed over 200 other individuals.

The mandate of the Commission was to review the efficacy and appropriateness of the activities of the US Intelligence Community (IC) in the post Cold War global environment and to make such recommendations as the Commission considered advisable. As required by law, the Chairman of the Commission—Dr. Harold Brown, former Secretary of Defense—submitted the report and its recommendations to the President and to the Congressional intelligence committees.

The Goal of the Report

This 200-page report contains a number of recommendations for action by the Executive and Legislative Branches that would, in the view of the Commission, produce a more effective, more efficient, and more responsive Intelligence Community to serve the nation's interests.

The unclassified report has concluded that the IC, with 14 separate agencies, is functioning well in its current form and performing a valuable service for the rest of the government. The report does, however, call for increased efficiencies in the organizations.

The Commission's View of Counterintelligence

The Commission stated that counterintelligence (CI) is a critical part of nearly all intelligence activities. When performed properly, the CI function is integral to the intelligence activity itself and part of the overall security of the organization. As the Ames case demonstrated, the consequences of poor CI can be disastrous and deadly.

In Chapter 2 of the report, the Commission first describes the basic CI functions of detecting and monitoring the activities of foreign intelligence services and investigating those suspected of espionage. CI, however, is an integral part of the entire intelligence process, and all agencies that undertake intelligence collection must be constantly on guard that what they collect is genuine. This requires continuous evaluation of their sources as well as the information gathered from them. Intelligence analysts who are familiar with the totality of information on a particular topic are often in a position to detect anomalies.

Three Overarching Themes

While the Commission's recommendations address a great many issues, there are three discernible overarching themes:

1. The need to better integrate intelligence into the policy community it serves. Intelligence cannot operate successfully in a vacuum. Its effectiveness is largely a function of its responsiveness, and its responsiveness is a function of the relationships it has with those it serves, from the President on down.

2. The need for intelligence agencies to operate as a "community." In times of crisis or war, intelligence agencies overcome the obstacles that separate them and pull together toward a common objective. By all accounts, it is in such situations that intelligence performs best. The challenge is to create the same level of performance in the absence of crisis.

3. The need to create greater efficiency. The Commission's report suggests a number of ways this might be done. Few will be easy. If the intelligence function is to retain its vitality, however, and if the confidence of the Congress and the public is to be restored, more rigor and modern management practices must be brought to the system.

The Commission concluded that intelligence agencies have not performed this crucial function very well. Virtually all have suffered severe losses because of a failure to recognize anomalous behavior on the part of their own employees. Some have also had problems recognizing anomalies in the behavior of their sources or in the appearance or actions of their targets. The Ames spy case revealed serious shortcomings in both categories.

In Chapter 6, the Commission concluded that, given the history of CI failures in CIA operations, the concern remains that the CI function may not have found its permanent place in CIA's overall foreign intelligence mission.

In Chapter 7, the Commission stated that the CI function is not readily amenable to budgetary trade-offs among the various agency CI staffs. However, they concluded that there is a need for an independent review of CI budgets to ensure that adequate resources are being allocated to this function consistent with national objectives and priorities. In the past, funding for CI activities has occasionally been a convenient place for agencies under budget pressures to find money for other activities. This must be assiduously prevented.

The Commission believes that funding for CI activities should remain a part of the National Foreign Intelligence Program. At the same time, it is useful to have the National Counterintelligence Policy Board (NACIPB) perform a separate review of CI budgets. This approach should provide assurance that funding is adequate to achieve national objectives and priorities as well as prevent CI funds being used for other purposes.

In the wake of the Ames case, the IC made sweeping changes to its CI infrastructure. A new NACIPB, which reports to the Assistant to the President for National Security Affairs, was created to coordinate CI activities and resolve interagency disagreements. In addition, the National Counterintelligence Center (NACIC) was created to share and evaluate information regarding foreign intelligence threats.

The Commission reported that the area of CI has undergone significant changes over the past two years. They question, however, whether these changes will have a long-term positive effect; the Commission believes it is still too early to evaluate this issue.

The Commission concluded that, because CI is so crucial to the success of the entire enterprise, the IC must sustain the renewed emphasis recently placed on this function. CI must be viewed not as an annoying intrusion, but rather as an integral part of the intelligence process. It must focus not only on protecting our own sensitive information but also equally on efforts to manipulate our collection and analysis through double agents or other means. This process requires a certain openness of mind and a willingness continually to balance the conclusions drawn from intelligence with the possibility of deliberate deception by a target.

Summary of the Commission's Key Recommendations

The Commission perceives four functional roles for intelligence agencies—collection, analysis, covert action, and CI—as well as a number of "missions" in terms of providing substantive support to particular governmental functions. In each of the 14 chapters of its report, the Brown Commission summarized its principal recommendations. Cited below are the Commission's key recommendations that are contained in each chapter.

Chapter 1. The Need To Maintain an Intelligence Capability

The Commission concludes that the United States should continue to maintain a strong intelligence capability. US intelligence has made, and continues to make, vital contributions to the nation's security. Its performance can be improved. Its can be made more efficient. But it must be preserved.

Chapter 2. The Role of Intelligence

The Commission concludes that a capability to conduct covert actions should be maintained to provide the president with an option short of military actions when diplomacy alone cannot do the job. The capability must be utilized only where essential to accomplishing important and identifiable foreign policy objectives and only where a compelling reason exists why US involvement cannot be disclosed.

Chapter 3. The Need for Policy Guidance

The Commission recommends a two-tier structure to carry out the institutional role of the National Security Council (NSC). A "Committee on Foreign Intelligence" should be created, chaired by the Assistant to the President for Nation Security Affairs and includes the DCI, the Deputy Secretary of Defense, and the Deputy Secretary of State. This Committee should meet at least semiannually and provide broad guidance on major issues. A subordinate "Consumers Committee," comprising representatives of the major consumers and producers of intelligence, should meet more frequently to provide ongoing guidance for collection and analysis and periodically to assess the performance of intelligence agencies in meeting the needs of the Federal Government.

Chapter 4. The Need for a Coordinated Response to Global Crime

The Commission recommends the establishment of a single element of the NSC—a Committee on Global Crime—chaired by the Assistant to the President for National Security Affairs and including, at a minimum, the Secretaries of State and Defense, the Attorney General, and the DCI to develop and coordinate appropriate strategies to counter such threats to national security.

For these strategies to be effective, the relationship between intelligence and law enforcement also must be substantially improved. In this regard, the Commission recommends:

1. The President should designate the Attorney General to serve as the spokesperson and coordinator of the law enforcement community for purposes of formulating the nation's law enforcement response to global crime.

2. The authority of intelligence agencies to collect information concerning foreign persons abroad for law enforcement purposes should be clarified by executive order.

3. The sharing of relevant information between the two communities should be expanded.

4. The coordination of law enforcement and intelligence activities overseas should be improved.

Chapter 5. The Organizational Arrangements for the IC

To improve the ability of the Director of Central Intelligence to manage the IC, the commission recommends that the current position of Deputy Director of Central Intelligence be replaced with two new deputies to the DCI: one deputy for the IC and one with day-to-day responsibility for managing the CIA. Both would be appointed by the president and confirmed by the Senate. The deputy for the CIA would be appointed for a fixed term. To give the DCI greater bureaucratic weight within the IC, the DCI would concur in the appointment or recommendation for appointment of the heads of national intelligence elements within the Department of Defense and would be consulted with respect to the appointment of other senior officials within the IC. The Directors of the National Security Agency and Central Imagery Office or its successor agency would be dual hatted as Assistant Directors of Central Intelligence for signals intelligence and imagery, respectively. Their performance in those capacities would be evaluated by the DCI as part of their rating by the Secretary of Defense. In addition, the DCI would be given new tools to carry out his responsibilities with respect to the intelligence budget and new authority over the intelligence personnel system.

Chapter 6. Central Intelligence Agency

To provide greater continuity in the management of the CIA, the Commission recommends that the Deputy DCI responsible for the CIA be appointed to a fixed term with an overall length of six years, renewable by the president at two-year intervals. To improve the quality of management, the Commission recommends a comprehensive approach to the selection, training, and career progression of CIA managers. Separate career tracks with appropriate opportunities for advancement ought to be provided for specialists who are not selected as managers. Clear guidelines should be issued regarding the types of information that should be brought to the attention of senior Agency managers, including the DCI and Deputy DCI.

Chapter 7. The Need for a More Effective Budget Structure and Process

The Commission recommends that the budget for national intelligence be substantially realigned. Programs grouping similar kinds of intelligence activities should be created under separate discipline

managers reporting to the DCI. For example, all signals intelligence activities would be grouped under the discipline management of the Director of the National Security Agency. These discipline managers also would coordinate the funding of activities within their respective disciplines in the defense-wide or tactical aggregations of the DOD, thus bringing greater consistency to all intelligence spending. The DCI should be provided a sufficient staff capability to enable him to assess trade-offs between programs or program elements and should establish a uniform, communitywide resource database to serve as the principal information tool for resource management across the IC.

Chapter 8. Improving Intelligence Analysis

The Commission recommends that intelligence producers take a more systematic approach to building relationships with consumers in policy agencies. Key consumers should be identified and consulted individually with respect to the form of support they desire. Producers should offer to place analysts directly on the staffs of consumers at senior levels.

The Commission recommends that the skills and expertise of intelligence analysts be more consistently and extensively developed and that greater use be made of substantive experts outside the IC. A greater effort also should be made to better harness the vast universe of information now available from open sources. The systems establishing electronic links between producers and consumers currently being implemented should be given a higher priority.

The Commission recommends that the existing organization that prepares intelligence estimates, the National Intelligence Council, be restructured to become a more broadly based "National Assessments Center." It would remain under the purview of the DCI but be located outside the CIA to take advantage of a broader range of information and expertise.

Chapter 9. The Need to "Right-Size" and Rebuild the Community

The Commission recommends the enactment of new legislation giving the most severely affected intelligence agencies a one-year window to "right-size" their work-forces to the needs of their organization. Such authority would be available only to the CIA and to intelligence agencies within the DOD that decide to reduce their civilian work force by 10 percent or more beyond the present Congressionally mandated level. Agencies that avail themselves of this authority would identify positions no longer needed for the health and viability of their organization. The incumbents of such positions, if close to retirement, would be allowed to retire with accelerated eligibility. If not close to retirement, they would be provided generous pay and benefits to leave the service of the agency concerned, or, with the concurrence of the agency affected, exchange positions with an employee not in a position identified for elimination who was close to retirement and would not be allowed to leave under the accelerated retirement provisions. New employees would be hired to fill some, but not all, of the vacancies created, providing the skills necessary to satisfy the current and future needs of the agency involved.

Four separate civilian personnel systems exist within the IC. These systems discourage rotation between intelligence agencies, which is key to functioning as a "community." In addition, many aspects of personnel and administration could be performed more efficiently if they were centralized.

The Commission recommends the DCI consolidate such functions where possible or, if centralization is not reasonable, issue uniform standards governing such functions. The Commission also recommends the creation of a single "Senior Executive Service" for the IC under the overall management of the DCI.

Chapter 10. Military Intelligence

The Commission did find that progress had been made in reducing duplication in military intelligence analysis and production, but that the size and functions of the numerous organizations performing these functions continued to raise concern. The Commission recommends that the Secretary of Defense undertake a comprehensive examination of the size and missions of these organizations.

The Commission recommends that the Director for Intelligence (J-2), who is now an officer assigned to the Defense Intelligence Agency, be constituted as part of the Joint Staff and be made responsible for providing intelligence support to joint war fighting and for

executing the functions of the Joint Chiefs of Staff as they pertain to intelligence.

The Commission also found that a problem continued to exist with respect to how information produced by national and tactical intelligence systems is communicated to commanders in the field. Many organizations and coordinating entities within DOD are working on aspects of this problem, but no one, short of the Secretary of Defense, appears to be in charge. The Commission recommends that a single focal point be established on the staff of the Secretary of Defense to bring together all of the relevant players and interests to solve these problems. It considers the Assistant Secretary of Defense (Command, Control, Communication, and Intelligence) to be the appropriate official for this purpose.

The Commission recommends that the clandestine recruitment of human sources, now carried out by active-duty military officers assigned to the Defense HUMINT Service, be transferred to the CIA, utilizing military personnel on detail from the DOD as necessary.

Chapter 11. Space Reconnaissance and the Management of Technical Collection

The Commission recommends greater international cooperation in space reconnaissance through expanded government-to-government arrangements as a means of dealing with both the vulnerability and cost of US space systems. In this regard, the Commission proposes a two-tier approach as a model for such collaboration. The Commission also recommends that the President re-examine certain restrictions on the licensing of commercial imaging systems for foreign sale in order to encourage greater investment by US firms in such systems.

The Commission endorses greater coordination between the space programs of the DOD and IC in order to achieve economies of scale where possible but recommends the National Reconnaissance Office be preserved as a separate organization.

The Commission endorses the creation of a National Imagery and Mapping Agency as recently proposed by the DCI and the Secretary of Defense.

Chapter 12. International Cooperation

The Commission recommends that the DCI and the Secretaries of State and Defense develop a strategy that will serve as the normal basis for sharing information derived from intelligence in a multinational environment.

Chapter 13. Cost of Intelligence

The Commission recommends a number of actions that it believes would, if implemented, reduce the cost of intelligence. In particular, the Commission believes that, until the IC reforms its budget structure and process, as recommended in Chapter 7, it will remain poorly positioned to identify potential cost reductions.

Chapter 14. Accountability and Oversight

The Commission recommends that the president or his designee disclose the total amount of money appropriated for intelligence activities during the current fiscal year and the total amount being requested for the next fiscal year. The disclosure of additional detail should not be permitted.

The Commission recommends a comprehensive review of these arrangements by the Intelligence Oversight Board to ensure effective performance of the oversight function.

Robert Chaegon Kim

(The following are excerpts from the Affidavit in support of the arrest warrant and search warrant on Kim filed in the US District Court, Eastern District of Virginia, Case Number:96-00791-m.)

Robert Chaegon Kim, an employee of the Office of Naval Intelligence ("ONI"), is knowingly and without authorization transmitting classified documents, including materials classified at the "Secret" and "Top Secret" level, to Baek Dong-Il, a Naval Attaché for the Republic of Korea (hereafter "South Korea"). According to ONI officials, Kim has a computer at his desk which allows him access go government information systems such as the Electronic Collateral Support System (ELCSS); this system contains documents that the Office of Naval Intelligence receives from other U.S. intelligence agencies, including

documents classified at the "Secret" and "Top Secret" level. Kim regularly searches the system to find classified documents relating to military, political and intelligence matters in the Asia-Pacific region. Kim copies and stores these documents in his work computer, removes classification markings, prints them on his office printer, and transmits them to Baek Don-IL.

This affidavit is not intended to be an exhaustive summary of the investigation against Kim, but is for the purpose of setting out probable cause in support of:

a. an arrest warrant for Robert Chaegon Kim for violations of Title 50, United States Code Section 783(a);

b. a search warrant for KIM's residence at 20765 Bank Way, Sterling, VA, in the Eastern District of Virginia;

c. a search warrant for KIM's workspace, located in Room 2D225 at the Office of Naval Intelligence on Suitland Road in Suitland, MD.;

d. a search warrant for KIM's vehicle, a dark red 1987 Volvo license plate BVY 893.

Pursuant to Executive Order 12958, information which, if disclosed without authorization, could reasonably be expected to cause "damage to national security," must be classified as Confidential and properly safeguarded. Information which, if disclosed without authorization, reasonably could be expected to cause "serious damage to the national security," must be classified as Secret and properly safeguarded. Information which, if disclosed without authorization, could reasonably be expected to cause "exceptionally grave damage to the national security," must be classified as Top Secret and properly safeguarded. When a classified document can be released to a particular foreign country, the originating agency will usually place markings at the top of the document to show that is releasable to that country.

Robert Chaegon Kim

A review of Robert Chaegon KIM's personnel file at the Office of Naval Intelligence shows that Kim was born on January 21, 1940 in Seoul, Korea. He became a naturalized American citizen in Baltimore, Maryland on May 21, 1974. Kim is employed as a computer specialist in the Maritime Systems Directorate of ONI, known as ONI-7, and has been employed by ONI since November 20, 1978. Kim has had a "Top Secret" security clearance, and access to "Sensitive Compartmented Information (SCI), since 1979. KIM's work involves classified information to such an extent that he physically works within a "Sensitive Compartmented Information Facility ("SCIF").

According to KIM's personnel file, KIM's primary job responsibility is to provide technical oversight regarding the design, development and maintenance of U.S. computer system known as the "Joint Maritime Information Element"(JMIE). This system monitors, tracks and stores information related to international maritime movement and maritime vessel identification. As a computer specialist, Kim does not ordinarily have duties relating to South Korea, though he has occasionally performed duties relating to that country under the specific direction of ONI officials.

(A review was made of) a document signed by defendant Robert Chaegon Kim entitled "Sensitive Compartmented Information Nondisclosure Agreement." In this document, Kim acknowledges that he has been granted access to Sensitive Compartmented Information as part of his employment, that any unauthorized disclosure of classified information is a violation of federal criminal law, and that any unauthorized disclosure of SCI information could irreparably injure the United States or provide an advantage to a foreign nation. In this signed document,

he agrees that he will never divulge classified information to anyone not authorized to receive it without prior written authorization from the United States.

According to information obtained from Department of State records, Baek Dong-Il is a Korean national, an O-6 Captain in the Korean Navy and an employee of the South Korean government. Baek arrived in the United States on October 1, 1994 to begin a three year tour as Naval Attaché assigned to the Embassy of the Republic of Korea. He works at the Embassy of South Korea in Washington, D.C. According to DMV and telephone records, Baek Dong-Il resides in Falls Church, VA, in the Eastern District of Virginia.

This affidavit will refer to information obtained from electronic surveillance, video surveillance and searches of KIM's workspace and mail. In each instance, the surveillance and searches were authorized by court order.

5/9/96 - Delivery of Documents

On or about May 1, 1996, video surveillance of KIM's workspace revealed Kim working on his computer while simultaneously creating a handwritten list, hereafter referred to as the "K list."

On or about May 5, 1996, the FBI conducted a court authorized search of KIM's work computer at KIM's workspace at the ONI in Suitland, MD. During the search, the FBI copied files stored on KIM's computer. One file, Titled "Baek.ltr" and dated 1/24/96, was a letter from Kim to Baek. In the letter, Kim offered his services to Baek and another South Korean official on the "OBU/OED business." (It is known) that the United States is involved in negotiations with South Korea to sell South Korea the "OBU" system, which is a computer software system used for tracking maritime vessels. (It is also known) that Kim has no official role in the negotiation or sale of this system. In the letter, Kim states that he hopes Baek has digested "the materials I have sent you" and warms him to "please be careful with these materials."

The May 5, 1996 computer search revealed that Kim had stored a number of "K" files, that is, files titled with as "K" followed by a number, such as "K10." Most of these "K" files contained copies of documents from agencies of the United States relating to North Korea, South Korea or other Asia-Pacific countries. Some of these "K" documents had their original classification markings removed. Using comparisons with the original documents, (it was determined), that at least some of these documents are classified at the "Confidential," "Secret" or "Top Secret" level. In addition to the "K" documents, there were other files containing U.S. agency documents relating to South Korea and other Asia-Pacific countries; some of these documents are also classified.

On or about May 7, 1996, video surveillance of KIM's desk at the Office of Naval Intelligence, Suitland, MD, revealed Kim working on his computer, moving to his left where his printer is located, and returning to his desk with papers in hand. While working on the computer, and while retrieving the documents, Kim was observed writing on a scratch pad similar to the one observed on May 1, 1996. This scratch pad contained a handwritten "K" list similar to the one found in his computer two days earlier, that, a list of numbers each preceded by the letter "K" such as "K-10." These activities went on for several hours. Kim placed the papers in a pile on his desk, and put the pile in an 8X11 manila envelope. Kim placed the envelope in his briefcase, and left work that day with the briefcase.

Video surveillance revealed a portion of three documents that were placed in the envelope. By comparing the surveillance photograph to an original document, (it was) determined that one document was a document found in the May 5, 1996 computer search of KIM's computer under the title "K10." This document is a United States agency document classified "Secret" which relates to North Korea. This classification heading had been removed from the copy seen on video surveillance. By comparing the surveillance photograph to an original document, (it was) determined that the second document is a document of a United States agency classified "Top Secret" which relates to North Korea. The classification headings were removed from the copy seen on video surveillance. The third document was unclassified.

On or about May 9, 1996, electronic surveillance revealed that Kim telephoned Baek, and stated that he had something for Baek. There was discussion about how the two could meet for a delivery of this item. Kim

indicated that lunch would be difficult because Kim would be bringing "this thing" along, and the two joked about mailing it. Baek gave Kim directions so that Kim could drive to his house, and told Kim to give the package to his son, who was mowing the law.

On 10 May, 1996, Baek called Kim back, confirming he received "it" yesterday.

Early June, 1996 - Delivery of Documents

On or about June 3, 1996, video surveillance of KIM's desk at ONI revealed Kim working on his computer, moving to his left where the printer is located, and returning to his desk with papers in hand. Video surveillance revealed that one of these documents was a U.S. agency document with classification markings removed. Using comparisons with an original document, (it was) determined that this document is classified "Secret."

On or about June 4, 1996, video surveillance of KIM's workspace revealed, inside KIM's open briefcase, a manila enveloped addressed to Baek at Baek's home address.

On or about June 12, 1996, electronic surveillance revealed that Baek called Kim at KIM's office, and thanked Kim, adding that "what was shown to me" was interesting. The two then discussed a matter pertaining to negotiations between the United States and South Korea on a particular project. Baek asked Kim a question relating to "what you sent me," referring to information that Baek had received from Kim earlier. Kim indicated that he could not answer the question without reviewing the "original text again." "When I sent that," Kim added, "I cut it all off and threw it away." Based on an investigation, (It is) believe that this is a reference to KIM's practice of cutting off classification markings, as well as other identifying information found at the beginning and end of U.S. agency documents, before delivering documents to Baek. This practice makes it easier for Kim to remove documents undetected from his office.

After this June 12, 1996 conversation, video surveillance later that day revealed that Kim placed a document on his desk belonging to the United States classified "Secret" concerning the same U.S.-South Korea project that Kim had discussed with Baek that morning. Later that same day, electronic surveillance revealed another telephone conversation between Kim and Baek. In this conversation, Kim told Baek he reviewed the message again. Kim then summarized to Baek four paragraphs in this "Secret" document. Each individual paragraph that Kim described to Baek is classified at the "Confidential" or "Secret" level.

On or about June 16, 1996, agents of the FBI and the Naval Criminal Investigative Service (NCIS) performed a search of KIM's office space. This search revealed a document in KIM's "burn bag," written in Korean, containing excerpts from the above described "Secret" document.

6/17/96 - Mailing of Documents

On or about June 17, 1996, video surveillance of KIM's workspace revealed portions of three documents on KIM's desk. By reviewing the video, (it was) determined that these documents belong to agencies of the United States, and relate to South Korea. By comparing these documents to original documents, (it was) determined that the documents were altered, in that their classification markings were removed. Two of the original documents are classified "Secret," and the third classified "Confidential." Video surveillance showed Kim picking up these documents and placing them in his briefcase. Several hours later, video surveillance detected Kim leaving work with his briefcase.

A review of the outside of mail sent from KIM's residence revealed that on June 17, 1996, an 8X11 manila envelope was mailed from KIM's residence in Sterling, Virginia, in the Eastern district of Virginia, to Baek at his residence in Falls Church, Virginia, in the Eastern District of Virginia. The envelope had a return address label listing KIM's name and address as the sender, and was large enough to hold the documents that Kim removed from his office earlier in the day.

8/3/96 - Mailing of Documents

On or about August 2, 1996, video surveillance of KIM's workspace revealed portions of these three documents belonging to agencies of the United States and relating to Asia-Pacific countries on KIM's desk. Kim later moved these documents into his briefcase, and left the office with that briefcase.

25. On or about August 3, 1996, a mail cover revealed an 8X11 manila envelope postmarked from the Eastern District of Virginia to Baek's residence in the Eastern District of Virginia. The envelope had a return address in the name of Robert Kim with KIM's home address. FBI personnel opened the envelope, and found two of the three documents seen by video surveillance on KIM's desk on August 2, 1996. By comparing the documents to the original documents, it was determined that the classification markings had been removed. Both documents belong to agencies of the United States and are classified "Secret." According to markings on the original documents, portions of one of those documents had already been released to South Korean officials, but the remaining information in those documents was not releasable to South Korea. FBI personnel placed the two documents back in the envelope and returned it to the mail for delivery to Baek. Video surveillance has periodically detected the third document on KIM's desk or in his open briefcase, and to the best of my knowledge Kim has retained this document. Based on the video surveillance, this third document has had classification markings removed, and is classified "Secret."

On or about August 7, 1996, electronic surveillance revealed that Baek called Kim and stated that "the material you had sent me was safety received with thanks."

8/14/96 - Mailing of Documents

On or about August 9, 1996, video surveillance revealed that Kim was printing numerous materials and placing them on the corner of his desk. Portions of three documents were visible to video surveillance, and comparison to original documents showed that all three documents belong to agencies of the United States and are classified "Confidential." All three documents contain information relating to countries in the Asia-Pacific region near South Korea. According to classification markings on the documents, none of these documents may be released to South Korea.

On or about August 12, 1996, video surveillance detected Kim pick up unidentified documents from his desk and place them in is briefcase. Kim later left his office with that briefcase.

On or about August 14, 1996, mail coverage revealed that Kim mailed an 8X11 manila envelope postmarked in the Eastern District of Virginia addressed to Baek at Baek's Fall Church, VA address. The enveloped had KIM's name and home address on the return label. FBI personnel opened and searched the envelope, finding the three documents seen on KIM's desk on August 9, 1996. The classification markings had been removed from these documents. FBI personnel returned these documents to the envelope for delivery to Baek.

On or about August 17, 1996, electronic surveillance revealed that Baek called Kim at his residence, and left a message that he "truly gratefully and satisfactorily received the material that you sent me."

8/16/96 - Mailing of Documents

On or about August 14, 1996, video surveillance detected Kim printing numerous materials at his desk, and eventually placing them in his briefcase.

On or about August 16, 1996, mail coverage revealed that Kim mailed an 8X11 manila envelope postmarked from the Eastern District of Virginia addressed to Baek at Baek's Falls Church, VA address. The envelope had Kim's name and home address on the return label. FBI personnel searched the envelope, finding six documents belonging to agencies of the United States, all relating to countries and activities in the Asia-Pacific region near South Korea. The classification markings had been removed from these documents. Comparison to original documents shows that four of the documents are classified "Secret," and the other two unclassified. According to the classification markings, none of the four classified documents were releasable to South Korea. The documents were placed back in the envelope for delivery to Baek.

A note written in Korean was attached to one of the above documents. The note stated: "Captain Baek, used all the stamps, still have the envelopes. Thanks."

On or about August 21, 1996, electronic surveillance revealed that Baek called Kim at work and stated that he received the items. Kim stated that he was saving items for Baek.

8/28/96 - Mailing of Documents

On or about August 27, 1996, video surveillance of Kim's workspace revealed Kim printing numerous documents and placing them on a pile on his desk. Portions of 17 documents were visible to video surveillance. All of these documents were United States

agency documents relating to South Korea and other countries in the Asia-Pacific region.

On or about August 28, 1996, mail coverage revealed that Kim mailed an 8X11 manila envelope addressed to Baek at his Falls Church, VA residence. The return address label on the envelope had Kim's name and home address. FBI personnel searched the envelope, finding 19 documents. Seventeen of these documents appeared to be identical to those documents viewed by video surveillance on August 27, 1996. Comparison to original documents showed that all but four of the 19 documents are classified, many at the "Secret" level; according to the classification markings on the original documents, only 4 of the classified documents are releasable to South Korea. Classification headings had been removed from the classified documents. At the request of a U.S. agency, one of the documents was removed from the package, and the remaining 18 documents returned to the envelope for delivery for Baek.

On or about August 28, 1996, electronic surveillance revealed a telephone conversation between Kim and Baek. Kim confirmed that he had received the stamps and envelopes that Baek had sent him. Kim told Baek that he sent a high volume of "very hot items" Baek yesterday, and urged Baek to be very careful with the contents. Kim told Baek that he removed security markings on the documents by computer. Baek assured Kim that he is careful with the documents, shredding them after he translates them.

On or about August 31, 1996, electronic surveillance revealed that Baek contacted Kim and stated he had received the package.

9/6/96 - Mailing of Documents

On or about September 4, 1996, video surveillance of Kim's workspace revealed that Kim printed numerous documents on the office printer and placed them on his desk. Later, he placed these documents in his briefcase, and left the office with this briefcase. Portions of documents were visible to video surveillance, which revealed that the documents belonged to agencies of the United States. The documents related to South Korea and the Asia-Pacific region, and comparison to original documents revealed that all but one of the documents are classified, many at the "Secret" level. According to classification markings on the original documents, none of the documents were releasable to South Korea.

On or about September 6, 1996, mail coverage revealed that an 8X11 manila envelope addressed to Baek at Baek's address in Falls Church, VA, was received at a post office in Falls Church, VA. The return address label on the envelope had Kim's name and home address. FBI personnel opened and searched the envelope, finding eleven documents which were observed on Kim's desk on September 4, 1996. Classification markings had been removed from the documents. At the request of a U.S. agency, two documents were removed from the envelope. The remaining nine documents were placed back in the envelope for delivery to Baek.

Based on review of video surveillance, one of the documents that Kim printed on September 4, 1996 was not in the September 6, 1996 envelope. By comparing video surveillance to an original, I determined that this document belongs to an agency of the United States and is classified "Secret."

On or about September 7, 1996, surveillance at a golf course in Fort Meade, MD revealed that Kim, Baek, and two high ranking South Korean naval officials met and played golf together.

9/9/96 - Telefaxing of Document

On or about September 9, 1996, electronic surveillance revealed that Baek called Kim at Kim's office. Kim thanked Baek for his hospitality during the golf outing, and offered Baek information relating to the South Korean military, which Baek expressed an interest in receiving. A few minutes later, electronic surveillance revealed that a telefax of a United States agency document classified "Confidential" relating to South Korea was sent from Kim's office to Baek.

According to Department of the Navy officials, Kim has had no official duty nor liaison responsibilities relating to South Korea during the time period covered by this affidavit, and has not been authorized to disclose classified documents to South Korean officials. According to ONI regulations, Kim must report any "continuing association" with foreign nationals to his employer. According to ONI officials, Kim has not disclosed his association with Baek.

Based on surveillance, (it is known) that Kim normally drives between his home in the Eastern District of Virginia and his office in a car which, according to Department of Motor Vehicles, he owns. This car is a dark red 1987 Volvo, license plate BVY 893 VA. (It is planned) to search this vehicle while it is located in the Eastern District of Virginia.

Based on the above facts, there is probable cause to believe that Robert Chaegon Kim, an employee of any agency of the United States, has knowingly communicated classified information to an agent of a foreign government, the Republic of Korea, in violation of Title 50, United States Code Section 783(a).

(It was) asked that his affidavit with its accompanying warrants and complaint (not attached herein) be kept under seal until Kim's arrest on the morning of September 25, 1996, so that Kim will not be alerted to the searches before they occur.

From physical surveillance, It is known that Kim frequently leaves his home before 6 a.m. The plan is to arrest Kim after he has left his home within a mile of his home. Permission is asked to search his home immediately after his arrest to prevent any chance that the occupants of the home could become aware of the arrest and destroy evidence.

NOTE: On May 7, 1997, Robert Kim pleaded guilty to a low-level espionage charge. As part of a plea bargain, prosecutors dropped a more serious spying charge that carried a maximum life sentence. According to a federal grand jury indictment, Kim gave South Korea seven documents related to national defense. Six of the documents were classified Secret and one was Confidential. At the court hearing, Kim admitted passing Defense Department and Statement documents to South Korean Navy Captain Baek Dong-Il, an attaché at the South Korean Embassy who was later recalled to Seoul.

Robert Stephan Lipka

Robert Stephan Lipka, age 50, 17 Dublin Drive, Millersville, Pennsylvania, was arrested on 23 February 1996 without incident by Special Agents of the Federal Bureau of Investigation and charged with espionage. The complaint and warrant that was filed in the Eastern District of Pennsylvania today, is the first time in the history of this judicial district that anyone has been charged with espionage.

The complaint states that, between the years 1964 and 1974, Lipka conspired to deliver, communicate, and transmit to officers and agents of the Soviet Union information relating to the national defense. While Lipka was in the US Army, assigned to the National Security Agency (NSA) at Ft. Meade, Maryland, he was assigned to the Collections Bureau that has since been renamed the Priority Material Branch. His principal assignment was to remove classified NSA national defense documents from teleprinters and distribute them to the appropriate departments.

In an affidavit of probable cause accompanying the criminal complaint, the FBI alleges that Lipka often secured these classified documents on his person to escape detection from NSA security and used a common espionage technique known as a deaddrop to transfer these documents to the KGB and then retrieve payment at a prearranged site. The affidavit states that Lipka also possessed special spy cameras to clandestinely photograph sensitive documents.

Lipka left the military and moved to Lancaster, Pennsylvania, in August 1967, where he attended college at a local university. The affidavit stated that Lipka took NSA documents with him when he left his Army position and that he met with Soviet representatives as late as 1974.

UNITED STATES DISTRICT COURT EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA
v.
ROBERT STEPHAN LIPKA,
A/K/A/ "ROOK"

Complainants's Statement of Facts Constituting the Offense or Violation

That, between in or around 1965 to in or around 1974, in Lancaster County, in the Eastern District of

Pennsylvania, and elsewhere, defendant ROBERT STEPHAN LIPKA, a/k/a "Rook," did unlawfully, knowingly and willfully conspire, combined, confederate and agree, with Peter Karl Fischer, Ingeborg Else Dora Fischer, and Artem Petrovich Shokin, who are not charged herein, and other persons known and unknown, to communicate, deliver, and transmit to the Soviet Union and to representatives, officers and agents thereof, information relating to the national defense, including but not limited to information directly concerning communications intelligence, with the intent and reason to believe that such information would be used to the injury of the United States and to the advantage of the Soviet Union, in violation of Title 18, United States Code, Section 794(c). Among the overt acts committed in furtherance of this conspiracy, in or around December 1968, after receiving a post card from a representative of the Soviet Union at his (Lipka's) residence, defendant LIPKA drove from Lancaster, in the Eastern District of Pennsylvania, to a location in the District to Maryland, to meet with a representative of the Soviet Union.

Affidavit Introduction: Deleted for brevity.

Robert Stephan Lipka and the National Security Agency (Highlights)

Robert Stephan Lipka was born on June 16, 1945, and enlisted in the U.S. Army on or about August 19, 1963. From October 1963 to January 1964, Lipka received Army training to be an intelligence analyst.

On December 30, 1963, Lipka was issued a "Top Secret" U.S. Government security clearance and received official authorization to have access to cryptographic U.S. government information.

On January 22, 1964, Lipka began working at NSA Headquarters at Fort Meade, Maryland.

From January 1964 to August 1967, Lipka worked in a NSA office which was known as the Collection Branch (CB) and was renamed the Priority Materials Branch (PMB) in October 1964.

From January 1964 to August 1967, the CB/PMB had two to four teleprinters dedicated to printing electrically transmitted classified reports. The CB/PMB also periodically received typewritten classified reports via courier from other DOD agencies and from other U.S. government agencies.

During this period, Lipka's principal assignment at CB/PMB was to remove the classified reports described above from the teleprinters and sort them for distribution to the appropriate NSA units. On occasion, he would also distribute the classified reports CB/PMB received via courier.

Lipka's military records show that in August 1967 he left active service and began residing in Lancaster, Pennsylvania.

Cooperating Witness

A cooperating witness (CW), advised s/he first met Lipka in 1965 and remained in frequent contact with him until the late 1970s. According to the CW, during the winter of 1966-67, Lipka admitted to the CW that he (Lipka) was taking things from NSA and selling them to the Russians. Lipka used the name "Ivan" to refer to his Russian contact.

The CW accompanied Lipka to a restaurant in Maryland during January 1967, where he delivered a package for "Ivan." Lipka told the CW he had placed a package in the toilet tank in the men's room. After placing the package, Lipka and the CW proceeded to a wooded area that night to retrieve a package of money. Lipka searched for the package but could not find it. He became frightened and they left the park hurriedly. The CW also remembers accompanying Lipka to other parks and fishing areas where Lipka would place or retrieve packages, usually wrapped in plastic and bound with tape.

In the summer of 1966, Lipka showed the CW three cameras, which he described as being used by spies to copy information. One was operated by being rolled over a document. The other two were very small; one was only an inch in height. At the time, Lipka told the CW that he had the cameras in connection with a NSA security project. (Note: There are no NSA or Army records of Lipka ever being assigned to any project that would require the use of these cameras.)

The CW stated that, after retrieving envelopes containing the money he was paid by the Russians for the NSA material he passed, Lipka would often count

it in CW's presence. The CW recalled that Lipka received approximately $500 in U.S. currency as payment, except for two occasions when he received $1000.

The CW described how, sometime in December 1968, after Lipka had moved to Lancaster, Lipka told the CW that the Russians had contacted him via post card and that he was considering meeting with them. Lipka was no longer working at NSA, but he told the CW he had retained NSA documents in order to keep his options open.

A few days later, the CW and Lipka traveled to a store in Maryland, where they were required to be at a specific time. Lipka took some NSA documents with him. At the store, Lipka left the CW alone for a few minutes and then returned, telling the CW that he had met with the Russians but that no agreement had been reached.

The CW advised that Lipka's recognition signal or code word that he used in communicating with the Russians was "*Rook*." Lipka said he had an emergency plan and that if he were every caught, the Russians would get him out.

Artem Shokin and the Fischers' (Highlights)

Peter Karl Fischer and his wife, Ingeborg Else Dora Fischer (nee Ziegler), lawfully entered the United States from Canada to reside in Buffalo, NY, in February 1965. They moved from Buffalo to Philadelphia in 1966, and then to Upper Darby, in the Eastern District of Pennsylvania. They both claimed they were born in 1929, in what later became East Germany.

According to official U.S. records, Artem Petrovich Shokin, a citizen of the Soviet Union, was employed by the UN Secretariat at UN Headquarters in New York City from 1965 to 1970.

On April 13, 1968, the Fischers traveled by car to New York City where they delivered unidentified items through use of a KGB dead drop near Grant's Tomb. Later that day, Shokin traveled to the same area, ostensibly to service the dead drop. The Fischers were later heard in a conversation in which they discussed their mission and congratulated themselves on their success.

Other evidence suggests the Fischers were acting at the behest of the KGB. A search of their apartment disclosed two short-wave radios. An examination of bank records on six occasions between August 1965 and November 1966 showed deposits to the Fischers' U.S. joint bank accounts from Switzerland. The Fischers' recorded conversations also revealed an anti-U.S. and pro-Soviet bias, and the use of terminology commonly associated with Soviet communism. This activity lead investigators to the conclusion that Peter Fischer was a KGB illegal officer posing as a German immigrant to the United States, and that Ingeborg Fischer was his knowing and willing assistant. It was further concluded that Shokin was a KGB officer operating under cover of an employee of the UN Secretariat.

The Fischers' Contact with Lipka

Based on recorded conversations and an analysis of travel patterns, there is strong evidence the Fischers made contact with Lipka on April 21, 1968. Six days later, a piece of paper in Fischers' apartment was annotated with the world "ROECK." There is no German word spelled R-O-E-C-K., but it could more or less be pronounced as "rook." As noted above, the CW stated that Lipka's codeword signals was *Rook*."

Undercover Investigation of Lipka

Between May 12 and December 8, 1993, an undercover FBI special agent, posing as "Segey Nikitin," an official of Russian military intelligence, had four meetings with Lipka and several instances of written correspondence.

Lipka was initially very uneasy with Nikitin because the special agent didn't know Lipka liked the game of chess or his code name. Before Nikitin was totally accepted, Lipka tested him in several areas involving his case history and past association with the KGB. The special agent was finally accepted, saying that the reason for his unfamiliarity with Lipka was because the case had been transferred from the KGB to the GRU.

Over time, Lipka and Nikitin discussed the circumstances and reasons for Lipka's breaks in contacts with the KGB, his access to and passage of materials to the Soviets, and his use of dead drops and meetings with his Soviet handlers.

Lipka pressed Nikitin for money for his prior espionage work, which he claimed he didn't receive due to missed drops. Lipka also said he still had documents he had taken from NSA and agreed to send them to Nikitin. He later said he took the NSA materials with him after he stopped working there in 1967.

The two men then began communicating through an accommodation address. Lipka was referred to as *en passant* (a chess term) and Nikitin was *Checkmate*. Lipka later told Nikitin he would refer to him as "*Carl Marx*," a variation on the initial letters of the word checkmate. Lipka later signed a letter to Nikitin as "*Enrico Passante*, " a variation on the initial letters of Lipka's parole. The term "coins" was used in reference to the NSA material. Lipka was paid $5,000 and told that additional payments would be made.

Throughout their meetings and correspondence, Lipka expressed mistrust and doubts about Nikitin, and Lipka refused on several occasions to comply with instructions, discuss his training, or clear dead drops in a timely manner. He also professed to a memory problem and frequently claimed he was underpaid for his efforts.

Lipka's final meeting with Nikitin was on December 8 1993, in Lancaster. Before this final meeting ended, Nikitin gave Lipka emergency contact instructions with a new accommodation name, address and telephone number, and $5000 as the balance due for his past espionage activities.

On September 15, 1994, the FBI mailed Lipka a copy of *The First Directorate*, by former KGB Major General Oleg Kalugin. At page 82 *et seq*., this book implicates Lipka in its detailed description of espionage committed by a "young soldier at NSA" who provided "reams of top secret material" to the KGB in the mid-1960s, prior to leave to go to college. In the letter, "Carl Marx" advised Lipka that if the need arises, he should activate the instructions for an emergency contact.

Conclusion

Based on the foregoing, the U.S. Government believed there was probable cause to believe that ROBERT STEPHAN LIPKA violated Title 28, United States Code, Section 794(c), conspiracy to commit espionage, as charged in the Criminal Complaint.

Note: On 23 May 1997, Robert S. Lipka pleaded guilty to one count of conspiracy to committee espionage and was sentenced to 18 years in prison and a fine of $10,000. The sentence came in a bargain for Lipka's plea of selling top-secret NSA documents for Soviet agents 30 years ago.

Phillip Tyler Seldon

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v. CRIMINAL NO. 96-305-A

PHILLIP TYLER SELDON,

Defendant.

CRIMINAL INFORMATION

The United States Attorney Charges That:

from on or about November 6, 1992 through on or about July 10, 1993, in the Eastern District of Virginia and elsewhere, PHILLIP TYLER SELDON, then an officer and employee of the United States and the Department of Defense, did unlawfully, willfully and knowingly conspire, combine, confederate and agree with an officer in the air force of El Salvador to communicate to a person whom SELDON knew and had reason to know was an agent and representative of a foreign government, information which had been classified by the President as affecting the security of the United States, with defendant SELDON knowing and having reason to known such information to been so classified, and without defendant SELDON having been specifically authorized by the President and the head of the Department of Defense to make such disclosure of such information, in violation of Title 50, United States Code, section 783(b).

Manner and Means

1. It was part of the conspiracy that defendant SELDON would use his authorized access to classified information to generate and gather classified documents in his office located in the Pentagon.

2. It was further a part of the conspiracy that defendant SELDON would remove classified documents from the Pentagon.

3. It was further a part of the conspiracy that defendant SELDON would deliver classified documents to an officer in the air force of the El Salvador through use of the U.S. Postal Service and by personally delivering the classified documents to the El Salvadoran air force officer in El Salvador.

Overt Acts

In furtherance of the conspiracy and in order to effect the objects and purposes thereof, defendant SELDON performed the following overt acts in the Eastern District of Virginia and elsewhere:

1. On or about November 6, 1992, in the Pentagon, within the Eastern District of Virginia, defendant SELDON mailed a package containing classified documents to El Salvador, with the intent that such documents would be delivered to an officer in the air force of El Salvador.

2. On or about May 31, 1993, in El Salvador, defendant SELDON personally delivered an envelope containing classified documents to an officer in the air force of El Salvador.

3. On or about July 10, 1993, in Stafford County, within the Eastern District of Virginia, defendant SELDON mailed a package containing classified documents to El Salvador, with the intent that such documents would be delivered to a officer in the air force of El Salvador.

All in violation of Title 18, United States Code, Section 371

/s/ 8/7/96 by AUSA Robert C. Chesnut.

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v. CRIMINAL NO. 96-

PHILLIP TYLER SELDON,

Defendant.

STATEMENT OF FACTS

1. On or about May 14, 1983, defendant PHILLIP TYLER SELDON was commissioned as an officer in the U.S. Army.

2. On each of three occasions, on or about February 5, 1986, on or about November 30, 1987, and on or about July 17, 1992, defendant SELDON executed a Classified Information Nondisclosure Agreement (CINA) in which he acknowledged receiving a security briefing concerning (a) the nature and protection of classified information, and (b) the procedures to be followed in ascertaining whether or persons to whom he might contemplate disclosing classified information have been approved access to it. In each CINA defendant SELDON further acknowledged that he would never divulge classified information unless he had officially verified that the recipient had been properly authorized by the United States government to receive such information, or unless he (defendant SELDON) had been given prior written notice of such authorization from the U.S. government. In each CINA defendant SELDON further acknowledges that he was aware and had been advised that the unauthorized disclosure of classified information may constitute a violation of Title 50, United States Code, Section 783(b).

3. From on or bout July 2, 1987, through on or about May 25, 1994, Defendant SELDON held a "Top Secret" U.S. government security clearance.

4. From on or about February 22, 1991, through on or about July 6, 1992, defendant SELDON served with the U.S. Army in El Salvador. While in El Salvador, defendant SELDON came to know a certain officer in the air force of El Salvador.

5. On or about July 7, 1992, defendant SELDON began serving with the U.S. Army in the Pentagon as a military assistant to a senior executive of the Department of Defense.

6. A few months later, the El Salvadoran air force officer telephoned defendant SELDON from El Salvador and asked defendant SELDON to provide him with certain information that the air force officer believed defendant SELDON had access to pursuant to his new job duties. On several other occasions before on or about July 10, 1993, the El Salvadoran officer and defendant SELDON had additional telephone conversations in which the El Salvadoran officer made additional requests for information from defendant SELDON.

7. On or about November 6, 1992, defendant SELDON mailed a package containing, among other things, an envelope in which were enclosed several documents containing classified information originating from the Central Intelligence Agency and/or the Department of Defense. Defendant SELDON had obtained the documents through his employment at the Pentagon. Defendant SELDON mailed the package from a post office in the Pentagon in the Eastern District of Virginia. The package was received in El Salvador by a U.S. official who, on SELDON's instructions, subsequently transferred it to the El Salvadoran air force officer, the U.S. official now knowing the package contained classified documents.

8. On or about May 31, 1993, defendant SELDON traveled to El Salvador, met with the El Salvadoran air force officer and delivered to him an envelope enclosing several documents containing classified information originating from the Central Intelligence Agency and/or the Department of Defense. Defendant SELDON had also obtained these documents by virtue of his employment at the Pentagon.

9. On or about July 10, 1993, defendant SELDON mailed a package containing, among other things, an envelope containing several documents containing classified information originating from the Central Intelligence Agency and/or the Department of Defense. Again, defendant SELDON had obtained the documents through his employment at the Pentagon. Defendant SELDON mailed the package from a post office in Stafford, Virginia, in the Eastern District of Virginia. The package was received in El Salvador by a U.S. official who, on SELDON's instructions, subsequently transferred it to the El Salvadoran air force officer, the U.S. official now knowing the package contained classified documents.

10. On at least one occasion, the El Salvadoran air force officer, upon receiving classified documents from defendant SELDON, provided the documents to other officers in the El Salvadoran air force. SELDON was unaware of this transfer.

11. The United States learned of the criminal conduct when SELDON applied for another position with the United States which required a polygraph examination as a prerequisite to employment. Over a period of time and in response to a series of questioning, SELDON disclosed his transmittal of classified documents, which the United States confirmed through mailing records and interviews with individuals in El Salvador.

12. While admitting to the offense conducted, SELDON has voluntarily reviewed numerous documents, and identified documents that he believes he transmitted to the El Salvadoran officer. Many of these documents were classified, and some were classified "Secret." SELDON identified one document, which was classified "Top Secret," as a document that he believes that he may have passed. However, he cannot specifically recall passing this document, and is unsure that he passed it. The parties agree that the United States cannot prove beyond a reasonable doubt that any document classified "Top Secret" was passed, but the parties agree that documents classified "Secret" and below were passed.

All of the above described actions of defendant SELDON were performed knowingly and willfully, not by accident or mistake. Had this case gone to trial, the United States would have proven SELDON's illegal conduct beyond a reasonable doubt.

The Nicholson Chronology

June 1994: Stationed in Malaysia, Nicholson begins his espionage career for the Russians. Just prior to his return to the United States, he has several meetings with his KGB handlers. Immediately after these meetings, he deposits $12,000 to his credit union account in Oregon.

December 1994: Nicholson takes a three-week vacation to Asia. During and after the trip, he deposits money into his account and pays off credit card debts; the amount totals $28,000.

June-July 1995: Nicholson takes another Asia vacation and shows $24,000 in unexplained deposits and payments.

October 1995: Nicholson's polygraph examinations shows deception to questions of unauthorized foreign contacts.

December 1995: Nicholson takes a Christmas vacation in Thailand and again $27,000 shows up in his bank account.

January 1996: A CIA internal investigation focuses on Nicholson. FBI agents assigned to CIA Hqs detect a pattern of foreign travel and unexplained income.

March 1996: A Russian intelligence officer informs an FBI agent that the Russian Government has issued a worldwide task to obtain information on terrorism by Chechnya rebels.

April 1996: Nicholson, who is an instructor at a CIA training facility, attempts to obtain information on Chechnya although he has no need to know.

June 1996: FBI has Nicholson under surveillance. Vacationing in Singapore, he is observed entering a Russian diplomatic vehicle. Following his vacation, he gives his son $12,000 to buy a new car and distributes another $20,000 for purchases, credit payments, and savings.

July 1996: Nicholson is assigned to the Counterterrorism Center at CIA Hqs. An audit of his computer use shows him searching databases not related to his job. He is listed as a surfer.

1 August 1996: Nicholson mails an envelope with a false return address and a greeting card inside with an alias name. The FBI believes he was signaling the KGB that he had a new assignment at CIA Hqs.

11 August 1996: FBI agents search Nicholson's Chevy van. His laptop computer hard drive is analyzed along with a diskette. Both are loaded with classified documents.

23 September 1996: Nicholson is caught photographing documents by a hidden camera in his office.

9 October 1996: Nicholson is observed using a mail drop to signal a meeting in Switzerland in late November with his Russian handlers.

23 October 1996: An FBI search of Nicholson's residence fails to uncover any new evidence.

3 November 1996: A search of Nicholson's office at CIA by FBI agents turns up 40 documents on Russia, none of which were pertinent to his work.

12 November 1996: Nicholson is again observed photographing documents in his office.

16 November 1996: The FBI arrests Nicholson at Dulles International Airport.

Respectfully submitted,

HELEN F. FAHEY
UNITED STATES ATTORNEY

BY: Robert C. Chesnut
Assistant United States Attorney
Michael C. Liebman, Trial Attorney
Internal Security Section
Criminal Division
U.S. Department of Justice

SEEN AND AGREE:
Phillip Tyler Seldon
Defendant

Joseph J. Bernard, Esquire
Counsel for the Defendant

(All signed: 8/7/96)

PLEA AGREEMENT HIGHLIGHTS

1. SELDON agrees to waive indictment and plead guilty to a one count criminal information filed with this agreement. The maximum penalty for this offense is five years of imprisonment, a fine of $250,00, full restitution, a special assessment, and two years of supervised release.

2. The Court may order the defendant to pay a fine sufficient to reimburse the government for the costs of imprisonment, term of release and probation, if so ordered.

3. The defendant is aware that his sentence will be imposed in accordance with the Sentencing Guidelines and Policy Statements. The U.S. makes no promise concerning what sentence the defendant will receive. The defendant waives his right to appeal the sentence.

4. The United States will not further criminally prosecute defendant for this specific conduct

5. The defendant represents to the Court that he is satisfied that his attorney has rendered effective assistance.

6. The defendant adopts the Statement of Facts and agrees that the facts therein are accurate in every respect.

Harold J. Nicholson

(*Excerts from the Affidavit in support of complaint, arrest warrant and search warrants update*)

United States v. Harold J. Nicholson

As more fully described below, Harold James Nicholson, an American citizen and employee of the Central Intelligence Agency (CIA), has been acting clandestinely, corruptly and illegally as an agent of the *Russia*n Federation Foreign Intelligence Service, Sluzhba Vneshney Razvedki Rossii, commonly referred to within the U.S. intelligence community as SVRR. The SVRR is the direct successor to the Committee For State Security of the Union of Soviet Socialist Republics (hereafter USSR), known as the KGB. By his actions, Nicholson has committed violations of 18 U.S.C. 794(a) and (c), that is, with reason to believe that it would be used to the injury of the United States and the advantage of a foreign nation, he has unlawfully and knowingly conspired to communicate, transmit and deliver to representatives of a foreign government, specifically the Russian Federation, information relating to the national defense of the United States. The investigation reveals that the Russian Federation has paid Nicholson over $100,000 since June, 1994 for his unlawful acts.

Information in this affidavit is based on my personal knowledge and on information provided to me by other law enforcement officers. This affidavit also relies on information provided by the CIA, which has cooperated with the investigation. This affidavit is not intended to be an exhaustive summary of the investigation against Nicholson, but is for the purpose of setting out probable cause in support of:

a. A complaint charging Harold J. Nicholson; with a violation of title 18, United States code section 794(c) (conspiracy to commit espionage);

b. An arrest warrant for Harold J. Nicholson;

c. A search warrant for Nicholson's residence at 5764 Burke Towne Court, Burke, Virginia, in the Eastern District of Virginia;

d. A search warrant for Nicholson's workspace, located in room 6E2911, Old Hq. Building, CIA Headquarters, Langley, Va;

e. A search warrant for Nicholson's vehicle, a 1994 *Chevrolet Lumina* sports van, Virginia license plate 8888BAT;

f. A search warrant for a safe deposit box in the name of Harold J. Nicholson, Box #417, located at Selco Credit Union in Springfield, Oregon.

g. A search warrant for any luggage that Nicholson may be carrying or may check at *Dulles Airport* on November 16, 1996, the day of his arrest.

Background

Harold James Nicholson, was born on November 17, 1950, in Woodburn, Oregon. He is divorced, and has three children. Nicholson entered on duty as an employee of the CIA on October 20, 1980. According to CIA records, Nicholson took the oath of office on January 26, 1982, where he stated that "I will support and defend the Constitution of the United States against all enemies foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. so help me God."

I have reviewed Nicholson's CIA personnel and security files. These files reveal that throughout Nicholson's employment with the CIA, he has held a "Top Secret" security clearance, and had regular, frequent access to sensitive classified information. I have also reviewed a document signed by Harold J. Nicholson entitled "sensitive compartmented information nondisclosure agreement." In this document, Nicholson acknowledges that he has been granted access to sensitive compartmented information (SCI) as part of his employment, that any unauthorized disclosure of such highly classified information is a violation of federal criminal law. and that any unauthorized disclosure of SCI information could irreparably injure the United States or provide an advantage to a foreign nation. In this signed document, Nicholson agrees that he will never divulge classified information to anyone not authorized to receive it without prior written authorization from the United States.

Harold J. Nicholson

In his career with the CIA, Nicholson has been assigned duties throughout the world. He has worked for the CIA as an operations officer specializing in intelligence operations against foreign intelligence services, including the intelligence services of the USSR and later, the Russian Federation. Specifically, from 1982-85, Nicholson worked for the CIA in Manila, where he had sustained, direct contacts with targeted Soviet officials. Nicholson worked for the CIA in Bangkok from 1985-87, and in Tokyo from 1987-89. From 1990-92, Nicholson was the CIA Chief of Station in Bucharest, Romania. From 1992 until 1994, Nicholson was the Deputy Chief of Station/operations officer in Kuala Lumpur, Malaysia, where, among other duties, he met with and targeted for recruitment Russian intelligence officers. From 1994 until July, 1996, Nicholson worked as an instructor at the classified CIA special training center ("STC") in the Eastern District of Virginia, teaching CIA trainees intelligence tradecraft. In July, 1996, Nicholson was assigned as a branch chief in the Counterterrorism Center, Directorate of Operations, at CIA headquarters in Langley, Virginia. this position carries a pay grade GS-15, and his current salary is approximately $73,000; it is the highest pay grade Nicholson has held during his CIA employment.

According to CIA records, Nicholson owns and currently resides in a townhouse at 5674 Burke Towne Court, Burke, Virginia, in the Eastern District of Virginia, Virginia department of motor vehicle records show that a *Chevrolet Lumina* sport van, Virginia plate no. 8888BAT, is registered to Harold J. Nicholson.

The Investigation–Polygraphs

On or about October 16, 1995, and October 20, 1995, Nicholson underwent polygraph examinations administered by CIA polygraphers as part of his routine security update. A computerized review of the examination results indicated a .97 (out of 1.0) probability of deception on two questions: (1) are you hiding involvement with a foreign intelligence service? and (2) have you had unauthorized contact with a foreign intelligence service? During one the examinations, a CIA polygrapher deemed Nicholson's response "inconclusive" to the following question: "are you concealing contact with any foreign nationals"?

On or about December 4, 1995, Nicholson underwent a third polygraph examination administered by a CIA polygrapher. A computerized review of the examination revealed an .88 probability of deception on the following questions: (1) since 1990, have you had contact with a foreign intelligence service that you are trying to hide from the CIA? and (2) are you trying to hide any contact with a foreign intelligence service since 1990? The CIA examiner noted that Nicholson appeared to be trying to manipulate the test by taking deep breaths on the control questions, which stopped after a verbal warning.

By reviewing CIA records and Nicholson's frequent flyer records and financial records from 1994 through early 1996, the FBI uncovered a pattern of twice yearly foreign travel, followed by unexplained deposits and payments to Nicholson's accounts.

June 1994 Meeting with Russian and Unexplained Money

According to CIA records, Nicholson was assigned to Kuala Lumpur, Malaysia during 1992-94 as Deputy Chief of Station/operations officer. CIA records show that Nicholson met with an officer of the Russian Intelligence Service SVRR in Kuala Lumpur on four occasions during Nicholson's final months there; three of these meetings took place in the Russian Embassy in Kuala Lumpur. These meetings were authorized by the CIA and reported by Nicholson. On June 30, 1994, one day after Nicholson's last reported meeting with the SVRR officer, financial records show that $12,000 was wired into Nicholson's savings account #000026-1759/01 at Selco Credit Union, Eugene, Oregon. Nicholson left Kuala Lumpur on July 5, 1994, and returned to the United States. The FBI has been unable to trace the source of this money to any legitimate source of income.

December 1994 Foreign Travel and Unexplained Money

According to Nicholson's travel records, Nicholson left the United States on personal travel on or about December 9, 1994. According to an itinerary he provided to the CIA, Nicholson planned to travel to London, New Delhi, Bangkok and Kuala Lumpur. Nicholson left Kuala Lumpur on December 28, 1994, returning to the United States on December 30, 1994.

According to financial records, after arriving in Kuala Lumpur, Nicholson made a $9,000 wire deposit from Malaysia to his Selco checking account #000026-1759/10, and a $6,000 cash payment to his American Express account #3728-128689-71001. Almost immediately after returning to the U.S., on December 31, 1994, Nicholson entered the Selco Credit Union in Eugene, Oregon, and, using 130 $100 bills, paid off a $3,000 loan at Selco (loan #86, Volkswagen), and paid $10,019.35 toward his Selco Visa account. The FBI has been unable to trace the source of the money in these transactions to any legitimate source of income.

June/July 1995 Foreign Travel and Unexplained Money

CIA leave records show that Nicholson took annual leave from June 15, 1995 through July 14, 1995. According to an itinerary Nicholson provided to the CIA, Nicholson left the United States on June 16, 1995, for Singapore, then traveled to Kuala Lumpur, where he stayed from June 17 through July 1, 1995. Nicholson returned to the United States through Hong Kong on July 1, 1995.

Analysis of financial records created during and shortly after the trip show the following financial transactions totaling $23,815.21 involving accounts in the name of Harold J. Nicholson and joint accounts he holds with his children. The FBI has been unable to trace these financial deposits and payments, which are set out below, to any legitimate source of income.

Date	Amount	Institution	Account
6/21/95	$6,300	American Express	3728-128689-71001
6/30/95	$1,000	Selco Credit Union money market	000026-1759/20
6/30/95	$4,715.21	Selco Credit Union Visa	4202-51000-261-7591
6/30/95	$1,000	Selco Credit Union	000029-1248
6/30/95	$1,000	Selco Credit Union	000034-2527
6/30/95	$1,000	Selco Credit Union	000029-1249
7/10/95	$1,000	Selco Credit Union checking	000026-1759/10
7/10/95	$1,000	Selco Credit Union money market	000026-1759/20
7/17/95	$3,000	Central Fidelity	7922119540
7/17/95	$1,000	Central Fidelity	7922119540
7/20/95	$1,400	USAA Mutual Fund	52900-468973
7/20/95	$1,400	USAA Mutual Fund	54900-278125

December 1995 Foreign Travel and Unexplained Money

According to CIA leave records and Nicholson's travel records, Nicholson left the United States for personal travel on December 18, 1995, and arrived in Bangkok, Thailand on December 20, 1995. Nicholson stayed in Bangkok until December 24, 1995, when he left for Phuket, Thailand. Nicholson returned to the United States on December 30, 1995.

Analysis of Nicholson's financial records during and shortly after this trip show the following financial transactions involving accounts in the name of Harold J. Nicholson totaling $26,900 which the FBI has been unable to trace to any legitimate source of income.

date	amount	institution	account
1/3/96	$4,000	Central Fidelity	7922119540
1/3/96	$4,400	Central Fidelity	7922119540
1/4/96	$3,000	Central Fidelity	7922119540
1/5/96	$1,900	Central Fidelity	7922119540
1/8/96	$1,000	USAA Mutual Fund	52900-468973
1/8/96	$1,000	USAA Mutual Fund	54900-278125
1/11/96	$ 900	Central Fidelity	7922119540
1/16/96	$2,000	Central Fidelity	7922119540
1/17/96	$1,400	Central Fidelity	7922119540
1/22/96	$ 900	Central Fidelity	7922119540
2/6/96	$1000	Central Fidelity	7922119540

June 1996 Meeting with Russians in Singapore and Cash Payment

On or about March 17, 1996, FBI officials were contacted by an SVRR liaison officer who asked for information about Chechnyan terrorism. The SVRR liaison officer added that his request was part of a global tasking by SVRR Headquarters to gather information about Chechnya.

On or about April 26, 1996, Nicholson traveled from his duty station at the CIA's special training center to CIA Headquarters in the Eastern District of Virginia. While at CIA headquarters, he asked several CIA employees for background information about Chechnya; Nicholson claimed that he needed the information for a training exercise at the training facility. However, according to CIA officials at the training facility, training exercises ongoing at that time were developed months in advance, and no training was planned or conducted regarding Chechnyan matters. Requests for changes to the exercises must be submitted to a board for review, and Nicholson did not submit any proposed changes.

According to CIA records, Nicholson left the United States on personal travel on June 25, 1996, arriving in Singapore on June 26, 1996. While Nicholson's checked luggage was searched and no evidence found, the FBI was unable to search Nicholson's carry on luggage, which included a camera bag.

At the time of his travel, Nicholson had applied for a position as CIA chief of station in a foreign country, and was being actively considered for that post.

Upon arrival in Singapore on June 26, 1996, Nicholson checked into the garden wing at the Shangri-La Hotel, where the cost of a room exceeds $300 per night.

Surveillance of Nicholson in Singapore on June 27, 1996, revealed that Nicholson left his hotel with his camera bag at approximately 10:11 a.m. for about four hours. During this four hour period, Nicholson made a "surveillance detection run," that is, a trip designed to detect surveillance. For example, Nicholson was observed taking numerous countersurveillance measures, such as backtracking his steps, watching glass panels of shops to look behind him, then entering and immediately exiting a subway station. During this excursion, Nicholson made no purchases and took no photographs.

Surveillance of Nicholson later on June 27, 1996, in Singapore revealed that Nicholson left his hotel with his camera bag at approximately 6:15 p.m., and retraced part of his route from earlier in the day, finally arriving at a subway station at 7:15 pm. Nicholson remained on the elevated area of the station until all other passengers had gone to the station's lower level. Nicholson then came down the escalator and sat on a stone seat at the end of the station near a taxi stand. After a few minutes, Nicholson got up and went back into the main concourse area of the station. While walking through the concourse area, he was met by a Caucasian male. The two men walked together toward a taxi stand. A car pulled up to the taxi stand. The trunk of the car opened, and Nicholson placed his camera bag in the trunk. Nicholson then got into the back seat of the vehicle. The vehicle bore diplomatic license plates which are registered to the Russian embassy in Singapore. The vehicle left the area. This meeting with Russian nationals was not authorized, nor did Nicholson report it to the CIA as required by agency regulations.

The next morning, on or about June 28, 1996, surveillance detected Nicholson leave his hotel and go to an American Express travel services center in Singapore, where he made an $8,300 cash payment to his American Express account. Several days later, Nicholson left Singapore for Bangkok, paying his $1,679.59 bill in cash.

On or about July 2, 1996, Nicholson left Bangkok for Honolulu with a female companion. In an August 21, 1996 letter to the CIA, Nicholson identified this woman as a foreign national currently residing in Thailand whom he intends to marry. According to a receipt found in a car search described below, Nicholson made a $762.93 cash payment to the Hanalei Bay Resort in Hawaii on July 5, 1996.

Records of Nicholson's financial transactions during and immediately after this Singapore trip reveal approximately $20,000 in purchases, deposits and payments. In addition, electronic surveillance has detected a telephone conversation between Nicholson and an acquaintance indicating that Nicholson gave his son approximately $12,000 to purchase a new car. I have seen a cash receipt found in Harold J. Nicholson's van dated July 12, 1996, issued to his son for $12,377.50 cash.

date	**amount**	**institution**	**account**
6/28/96	$8,300	American Express	3728-128689-71001
7/1/96	$ 820.58	Overseas Union Bank purchase gold coins	
7/1/96	$1,679.59	Shangri La Hotel	
7/5/96	$ 762.93	Hanalei Bay Resort	
7/8/96	$1,000	Selco Credit Union	000029-1248
7/8/96	$1,000	Selco Credit Union	000034-2527
7/14/96	$ 120	Dulles Airport parking	
7/29/96	$5,000	Selco Credit Union	000026-1759/10

Nicholson's Move to CIA Headquarters

On or about July 16, 1996, Nicholson reported to his new position at CIA headquarters in the Counterterrorism Center. Nicholson had applied for several foreign postings, including the chief of station position discussed above, all of which were denied.

On or about July 19, 1996, an audit of CIA computer information revealed that Nicholson was using his computer to conduct searches in CIA databases for information using the following key words:"Russia(n)" and "Chechnya." As a result of Nicholson's use of these key words to conduct searches, CIA cables, reports, and documents containing either of those key words would be routed to his computer where he could read them and print them. According to CIA officials, Nicholson has no need for such materials in his present position.

The audit also revealed that Nicholson attempted to access CIA databases that he had no authorization to access, including two attempts to access Central Eurasian Division databases which would contain information on Russia. This unauthorized activity led the CIA computer security personnel to list Nicholson as a "surfer."

On or about August 1, 1996, surveillance detected Nicholson approach a mailbox at 8283 Greensboro Drive, Tyson's Corner, in the Eastern District of Virginia. A sealed Hallmark greeting card envelope containing a postcard was subsequently retrieved from the mailbox A return address of 2206 Pimmit Run, Falls Church, 22041 was hand-printed on the envelope. Both the envelope and the postcard carried oversized commemorative stamps with a face value on $1, an amount in excess of the necessary postage. The postcard, which was addressed to a post office box in a foreign country, contained the following text:

Dear J. F.,

Just wanted to let you know that unfortunately I will not be in your neighbor as expected. Priorities at the home office resulted in my assignment to the management position there. Some travel to your general vicinity to visit field offices will occur, but not for more than a few days at a time. Still, the work at the home office should prove very beneficial - I know you would find it very attractive. I look forward to a possible ski vacation this winter. Will keep you informed. Until then, your friend,

Nevil R. Strachey

P.S. I am fine.

Investigation at 2206 Pimmit Run, Falls Church, Virginia, revealed no one at this address named Nevil R. Strachey. The zip code 22041 is not accurate for 2206 Pimmit Run, Falls Church. No listing for Nevil R. Strachey was found in telephone directories for Northern Virginia, the District of Columbia, Prince George's and Montgomery County (MD).

(It is believed) the foreign post office box to which the postcard was mailed is an "accommodation address." An accommodation address is a prearranged address where an intelligence officer can receive mail clandestinely from an agent. The accommodation address itself may be serviced by an intermediary. This post office box appears to be the method that Nicholson uses to communicate with his SVRR handlers. The contents of the postcard appear to inform the SVRR that Nicholson did not get the particular chief of station foreign posting that he had sought, but instead got a management position at CIA Headquarters.

Classified Documents Recovered From Nicholson's Notebook Computer

On or about August 11, 1996, the FBI conducted a search of a 1994 Chevrolet Lumina sports van which is registered to Nicholson; surveillance and DMV records confirm that this is Nicholson's only vehicle. In addition to cash receipts confirming some of the above financial transactions, the FBI discovered a personally-owned notebook computer in the van. An analysis of the hard drive showed that it contained numerous CIA classified documents relating to Russia. All of these files had been deleted from program directories, which in my training and experience indicates that they had already been copied on to a disk and transmitted to Russian Intelligence. This is corroborated by the fact that the original classified documents are all dated prior to Nicholson's June 1996 trip to Singapore. While the files had been deleted, the FBI recovered certain files and fragments of files from the notebook computer's hard drive. A brief summary of some of these documents follows:

a. A fragment recovered by the FBI describes the planned assignment of a CIA officer to a position in Moscow. Nicholson trained this officer at a CIA training facility. The text of the fragment includes the statement "(comment: please see biographic profile prepared previously on (name of officer) as well as updated assignment listings provided separately." According to the CIA, information about this officer's assignment was classified "Secret." The assignment was intended to be a covered slot, and the officer was trained in the use of a full range of intelligence collecting techniques. Collection targets included, but were not limited to, military preparedness of the Russian Federation, the Russian Federation's knowledge of U.S. national defense plans, and other important foreign intelligence and counterintelligence matters. The disclosure of this officer could have led to the losses of human sources and caused

serious damage to U.S. intelligence capabilities. Further, the fragment indicates that Nicholson has provided the SVRR with biographic information and assignment listings of CIA case officers. This is confirmed by the fact that the hard drive also contained biographic information about CIA employees who were at the training facility during Nicholson's tenure there. Nicholson's position as a staff instructor at the CIA's special training center gave Nicholson access to highly sensitive information, including access to the biographical information and assignments for every CIA case officer trained during his two year tenure there. As a result of this disclosure, it will be difficult, if not impossible, for the CIA to place some of these newly trained case officers in certain sensitive foreign postings for the rest of their careers. Further, Nicholson communicated with other case officers who were instructors at the center, and may have heard descriptions of their work as part of training. The methods of training, and the techniques taught to future case officers, would be valuable information for foreign intelligence agencies.

b. A document concerning a closed briefing on Russian recruitment pitches to CIA case officers in the field. A CIA official has told the FBI that there was a briefing concerning recruitment pitches by Russian intelligence officers and that the briefing was classified "Secret." A CIA official said that information concerning how many recruitment pitches have been reported by CIA officers to CIA headquarters is classified "Secret."

c. A document concerning information on Chechnya. The information was a near verbatim copy of an actual "Secret" CIA report regarding Chechnya that had been provided to Nicholson by CIA officials. I believe that Nicholson gathered the Chechnyan information found on his computer in response to clandestine tasking from the SVRR, consistent with the SVRR's global tasking for such information as discussed above.

d. A document which included the statement "the following added notes were taken by me from the secret report from the CIA's Paris accountability review team, dated 16 June 1995...." According to a CIA official, the notes contained in the electronic document came from a "Secret" CIA report dated June 16, 1995 regarding expulsions of CIA officers from Paris.

e. A document regarding information about the Moscow CIA station. The document gave the name of the Chief of Station, and set out staffing information for this CIA office. CIA officials advised that information concerning the location and staffing of any CIA station is classified "Secret." (It is known) that the Russian intelligence services attempt to identify U.S. intelligence officers to identify CIA intelligence operations and confidential human assets, some of whom report on the military intentions and military preparedness of foreign powers.

f. A document summarizing information obtained during the debriefing of convicted spy Aldrich Ames.

g. An extended description of Nicholson's polygraph examination, focusing on the questions Nicholson had been asked about any unauthorized contact with a foreign intelligence service and the CIA polygraphy's reaction to the test.

A 3.5 inch computer diskette was also found in the search of the vehicle. Unlike the hard drive, it contained an electronic document that had not been erased titled "Subject: Reporting From Access Agents to Russian Sources and Developmental." Access agents are individuals who are not employed by the federal government. Instead, they are individuals who work in a variety of private fields who, by the nature of their work, often travel and gain valuable intelligence information. These individuals voluntarily provide this information to the United States. The identity of these assets is classified, as they could be the target of reprisals if foreign countries were aware of their intelligence gathering activities. The access agent document contained seven summary reports concerning CIA human assets and their confidential reporting on foreign intelligence matters. The document noted: (comment: The following was gleaned from reporting accessions lists on Russian objectives.): the topics included intelligence information concerning the Russian banking system, efforts of a foreign country to acquire

Russian cruise missile technology, acquisition of Russian designed electric field suppression systems of interest to the U.S. Navy, sound-vibration insulation for diesel generator plants, high frequency radar research, submarine weapons systems design, and information concerning the Russian economy. In addition, the human sources of information, whose identities the DIA seeks to protect from disclosure, were identified in the document by their codenames, positions, and access to particular information. CIA officials told the FBI that the seven items were all apparent extracts from three actual CIA documents, each dated July 18, 1996, and classified "Secret." A CIA official who examined the extracts said that the information contained in the extracts was classified "Secret" and consisted of Russian matters selected from a broader compilation of CIA headquarters comments to three CIA stations concerning reporting by CIA assets of those CIA stations. The "comment" reported above was not found in the text of any of the three CIA documents.

(It is known) that agents of foreign intelligence services collect information on computers and transfer the information on diskettes. I know that classified CIA intelligence information concerning staffing in Moscow; reports from CIA assets about Russian banking, technology, and political information; and information about the number of Russian recruitment pitches reported by CIA officers is valuable intelligence information which is being sought by the Russian intelligence services, particularly the SVRR. Much of the information on the hard drive and the disk relates to the national defense of the United States.

On or about August 24, 1996, a search of Nicholson's safe deposit box #417 at Selco Credit Union in Springfield, Oregon, revealed a number of gold and commemorative coins, including the two gold coins Nicholson purchased in Singapore with cash on July 1, 1996.

Nicholson's Planned Meeting with Russians in November 1996

On or about September 23, 1996, electronic surveillance at Nicholson's workplace in Langley, Virginia revealed Nicholson removing a camera from his desk and holding it above papers on his lap, as if he were trying to photograph documents. Nicholson had requisitioned this camera and lenses from the CIA. Later, Nicholson asked for a camera that folds down into a briefcase; ...this style camera is useful in photographing documents. According to CIA officials, Nicholson has no need for any camera in connection with his current official duties

On or about October 4, 1996, Nicholson made plans to travel to two foreign locations for official meetings with friendly foreign intelligence services, departing on November 16, 1996, and returning to the U.S. on November 26, 1996. Nicholson has informed travelling companions from the CIA that he plans to travel to Switzerland after the official meetings rather than return to the U.S. with them. Nicholson has made reservations to fly to Zurich, Switzerland.

On or about October 9, 1996, FBI surveillance observed Nicholson deposit an item in a mailbox at Gallows Road and Electric Avenue, Dunn Loring, Virginia. The FBI retrieved the item, a sealed airmail envelope which contained a postcard mailed to the same address and same foreign post office box as the August 1, 1996, postcard. Both the envelope and the postcard carried the same oversized commemorative style stamps with a face value of $1 as used on the August 1, 1996 postcard. The text of the postcard reads:

Hello Old Friend,

I hope it is possible that you will be my guest for a ski holiday this year on 23-24 November. A bit early but it would fit my schedule nicely. I am fine and all is well. Hope you are the same and can accept my invitation.

Best regards,
Nevil R. Strachey

P.S. The snow should be fine by then.

(It is believed) that Nicholson was informing an SVRR intelligence officer of his intention to meet in Switzerland on November 23 and November 24, 1996. (It is further believed) that the reference to "a bit early" refers to the fact that their prior semi-annual meetings have occurred in December.

On or about October 23, 1996, the FBI conducted a surreptitious search of Nicholson's residence. This search was very limited in that the FBI had little time to perform the search, and had to leave no trace of their

entry or the search. Most of the search focused on Nicholson's home and notebook computers, which revealed no new evidence. They each revealed that Nicholson keeps his notebook computer in his bedroom, and electronic surveillance has detected the sounds of typing in the bedroom at night. The search also revealed that Nicholson has an electronic document scanner at home which would enable him to scan documents onto a computer disk.

On or about November 3, 1996, FBI agents conducted a search of Nicholson's office in Langley, Virginia. Approximately 40 documents relating to Russia were found on his desk, including documents classified at the "Secret," "Top Secret," and "SCI" levels. According to CIA officials, these documents contained information concerning,among other things, the intelligence capabilities and military preparedness of the Russian federation. The documents do not appear to be germane to Counterterrorism Center matters. Many of these documents relate to the national defense of the United States. The majority of these documents was located in a black folder on his desk.

Unlike his computer at previous CIA assignments, Nicholson's computer at Langley has no disk drive. This security feature makes it impossible for anyone to copy classified documents onto a disk for editing, removal or transfer.

On or about November 9, 1996, electronic surveillance of Nicholson's workspace revealed Nicholson removing documents from the black folder on his desk, and removing classification markings from the tops and bottoms of documents. I believe that the no disk drive security feature of Nicholson's computer is forcing Nicholson to print out these documents and edit them by hand.

On or about November 12, 1996, in response to Nicholson's request, individuals from the CIA's Office of Technical Services delivered a document camera to Nicholson's office. Immediately Nicholson closed his door and placed the camera under his desk. Nicholson took some of the documents relating to Russia from the black folder, placed them under the desk, knelt on the floor, and began photographing the documents. Nicholson photographed documents for about 30 minutes on the morning of November 12, 1996. Surveillance detected Nicholson photographing documents under his desk later that same evening, and on the morning of November 13, 1996.

According to a personal financial statement that Harold J. Nicholson signed and filed with the CIA in 1995, Nicholson has no outside business interests or sources of income that account for the income described in connection with his foreign travel. His federal tax returns for the 1994 and 1995 tax years do not appear to declare the income described above that Nicholson has deposited in his accounts or used to pay debts.

Based on the above information, there is probable cause to believe that Nicholson is engaged in a conspiracy to commit espionage in violation of Title 18, United States Code Section 794 (c).

Items to be Searched for and Seized

a. Agents of foreign intelligence services maintain national defense and classified documents and materials, clandestine communications devices and instructions, contact instructions, codes, telephone numbers, maps, photographs, other papers and materials relating to communications procedures, proceeds of illegal espionage transactions, records, notes, bank records, financial statements, calendars, journals, and other papers or documents relating to: 1) the transmittal of national defense and classified intelligence information to foreign governments and intelligence services; 2) the identities of other foreign espionage agents and intelligence officers; 3) financial transactions including payments from governments and hidden financial accounts; 4) records of previous illicit espionage transactions; 5) the source and disposition of national defense and classified intelligence information.

b. Agents of foreign intelligence services often utilize espionage paraphernalia, including devices designed to conceal and transmit classified and intelligence information. These paraphernalia and devices include materials used by espionage agents to communicate between each other and with a foreign government, such as computer disks or photographic film.

c. It is common for agents of foreign intelligence services to secrete national defense and classified documents and materials, clandestine communications devices and instructions, contact instructions, codes,

telephone numbers, maps, photographs, other papers and materials relating to communications procedures, proceeds of illegal espionage transactions, records, notes, bank records, financial statements, calendars, journals, espionage paraphernalia, and other papers or documents on their persons and in secure, hidden locations and compartments within or near their residences, at places of employment, in safe deposit boxes, and in motor vehicles, including hidden compartments within motor vehicles, for ready access and to conceal such items from law enforcement authorities.

d. Agents of foreign intelligence services routinely maintain or conceal in and near their residences or in safe deposit boxes large amounts of U.S. and foreign currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of illegal espionage transactions. They also conceal records relating to hidden foreign and domestic bank and financial accounts, including accounts in fictitious names.

e. Agents of foreign intelligence services are not unlike any other individual in our society in that they maintain documents and records. These documents and records will normally be maintained for long periods of time regardless of whether their value to the agent has diminished. These persons maintain documents and records which will identify and corroborate travel both in the U.S. and abroad made in connection with clandestine espionage activity, including personal meets with foreign intelligence officers. These documents and records include passports, visas, calendars, journals, date books, telephone numbers, address books, credit cards, hotel receipts, airline records, correspondence, carbon copies of money orders and cashier's checks evidencing large cash expenditures, and accounts and records in fictitious names.

f. Agents of foreign intelligence services often maintain and conceal identity documents, including those utilizing fictitious identities, U.S. and foreign currency, instructions, maps, photographs, U.S. and foreign bank account access numbers and instructions, and other papers and materials relating to emergency contact procedures and escape plans.

Description of Items and Places to be Searched

(It is planned to) arrest Nicholson on November 16, 1996 at Dulles Airport in the Eastern District of Virginia just prior to his scheduled departure. In his past travel, Nicholson has checked luggage with the airline and also carried, hand luggage, including a camera bag, onto the airplane. Based on the above information, there is probable cause to believe that Nicholson will have classified information in some form on his person or secreted in his luggage for delivery to his SVRR handlers. Accordingly, should Nicholson check any items with the airline for transportation with his flight, or should he have any carry on items prior to boarding the aircraft.

NOTE: On 31 March 1997 Harold J. Nicholson, the highest-ranking CIA agent ever charged with spying for Russia, pled guilty to espionage. Nicholson admitted to a federal court that he sold Top-Secret U.S. intelligence information to the Russians for $180,000. On 5 June 1997, Nicholson was sentenced to 23½ years in prison. He did not get life imprisonment because of his cooperation with federal authorities.

Pitts Affidavit

Subject: Earl Edwin Pitts Affidavit
Category: Pitts Case

The following information is UNCLASSIFIED.

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

UNDER SEAL
UNITED STATES OF AMERICA

CRIMINAL COMPLAINT
v.
CASE NUMBER: 96-1041-M

EARL EDWIN PITTS
(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state the following it true and correct to the best of my

knowledge and belief. From on or about July, 1987 - December, 1996 in Arlington and Stafford Counties in the Eastern District of Virginia Defendent(s) did, (Track Statutory Language of Offense)

commit a violation of Title 18, U.S.C. Section 794 (c), that, with reason to believe that it would be used to the injury of the United States and the advantage of a foreign nation, Earl Edwin Pitts did unlawfully and knowingly conspire with others to communicate, transmit and deliver to representatives of a foreign government, specifically the U.S.S.R. and the Russian Federation, information relating to the national defense of the United States, and did overt acts to effect the object of said conspiracy, including but not limited to the following: Earl Edwin Pitts did travel on March 24, 1992 from National Airport, in the Eastern District of Virginia, to New York City; and did

commit a violation of Title 18, U.S.C. Section 794 (a), that is, with reason to believe that it would be used to the injury of the United States and the advantage of a foreign nation, Earl Edwin Pitts did unlawfully and knowingly attempt to communicate, transmit and deliver to representatives of a foreign government, specifically the Russian Federation, information relating to the national defense of the United States; and did

commit a violation of Title 50, U.S.C. Section 783 (a), that is, communication of classified information without authority by Government officer or employee to a person he had reason to believe was an agent of a foreign government; and did commit a violation of Title 18, U.S.C. Section 641, that is, conveyance without authority of property of the United States.

Earl Edwin Pitts

In violation of Title 18 United States Code, Section(s) 794 (a) and (c), and 641, and Title 50, U.S.C. § 783(a).

I further state that I am a Special Agent, FBI and that this complaint is based on the following facts:

_____

Signature of Complainant
David G. Lambert, Special
Agent Federal Bureau of Investigation

Reviewing AUSA - Randy I. Bellows
Sworn to before me and subscribed in my presence,
December 17, 1996 at Alexandria, Virginia

Date _____ City and State _____

Thomas Rawles Jones, Jr.
United States Magistrate Judge

Name & Title of Judicial Officer

_____

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT, ARREST WARRANT, AND SEARCH WARRANTS

UNITED STATES v. EARL EDWIN PITTS

I, David G. Lambert, being duly sworn, depose and state as follows:

1. I am presently employed as a Special Agent of the Federal Bureau of Investigation (FBI) and am assigned to the Washington Field Office in the District of Columbia. I have been employed as an FBI Special Agent for approximately 9 years. I have been assigned to foreign counterintelligence (FCI) investigations for approximately 7 years. As a result of my training and experience, I am familiar with the tactics, methods, and techniques of foreign intelligence services and their agents.

2. This affidavit is in support of the following:

a. Complaint and Arrest Warrant for:
EARL EDWIN PITTS,
DOB: September 23, 1953
SSAN: 486-62-7841,

for the following violations of federal criminal law.

a. Conspiracy to commit espionage (Title 18, United States Code, Section 794(c)); and

b. Attempted Espionage (Title 18, United States Code, Section 794(a)); and

c. Communication of Classified Information by Government , Officer or Employee (Title 50, United States Code, Section 783(a)).

3. The information stated below is based on personal knowledge, training and experience, including training and experience I have gained while assigned to FCI investigations, and information provided to me by others as noted herein.

Summary

4. This affidavit concerns an investigation by the FBI into the compromise of FBI intelligence operations and information. During this investigation, I and others have conducted interviews, physical and electronic surveillance, financial analysis, and other forms of investigation.

5. The results of this investigation to date indicate there is probable cause to believe that:

a. EARL EDWIN PITTS (hereafter, "PITTS"), a United States citizen, is an agent of the Sluzhba Vneshney Rasvedi Rossii (hereafter, "SVRR"), which is the intelligence service of the Russian Federation. The SVRR is the direct successor of the Union of Soviet Socialist Republics' Committee for State Security, known hereafter as the "KGB." An agent of a foreign intelligence service is one, other than an intelligence officer or employee, who clandestinely and illegally acts on behalf of that service. Prior to being an agent of the SVRR, there is probable cause to believe PITTS was an agent of the KGB.

b. From in or about July, 1987, through the present, PITTS conspired with officers of the KGB and SVRR to commit espionage. This included numerous trips which PITTS made from the Eastern District of Virginia to the New York area in connection with his espionage activities. From in or about October, 1992, to the present, to the best of my knowledge and belief, PITTS remained an agent of the SVRR in a dormant capacity.

c. During PITTS' espionage activities between 1987 and 1992, PITTS received from the KGB and SVRR in excess of $224,000, including over $100,000 set aside for PITTS in a "reserve" account (according to PITTS).

d. From in or about August, 1995, through the present, PITTS attempted to commit espionage and committed numerous other violations of federal criminal law in connection with his contact with certain individuals who he believed were agents of the SVRR but who were, in fact, undercover personnel employed by, or operating on the instructions of the FBI. During this "false flag" operation, described in greater detail below, PITTS gave persons he believed to be SVRR officers sensitive and Secret classified documents related to the national defense, gave "SVRR [FBI]" handlers personal, medical and family information about fellow FBI special agents, proposed strategies by which the SVRR might recruit additional agents, made plans to smuggle into the FBI Academy an SVRR technical expert, provided his "SVRR [FBI]" handlers an FBI cipher lock combination, an FBI key and his own FBI identification badge in order to facilitate the smuggling operation, stole from the FBI a handset to a telecommunications device used to transmit classified information, and divulged a variety of classified information to his "SVRR [FBI]" handlers. PITTS did this for money. During the "false flag" operation, PITTS accepted $65,000 for his espionage activities and his attempt to compromise FBI intelligence activities.

Background on Earl Edwin Pitts

6. EARL EDWIN PITTS is a United States citizen, presently employed as a Supervisory Special Agent of the FBI. PITTS is 43 years old and is an attorney. PITTS and his wife, Mary, were married in 1985. PITTS resides with his wife at a single family dwelling located at 13415 Fox Chase Lane, Spotsylvania, Virginia, 22553.

7. On September 18, 1983, PITTS entered on duty with the FBI and, on September 19, 1983, took the following Oath of Office:

> I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter. So help me God.

8. On September 20, 1983, PITTS signed an FBI Employment Agreement, which included the following provisions:

> That I am hereby advised and I understand that Federal law such as Title 18, United States Code, Sections 793, 794, and 798 . . . prohibit loss, misuse, or unauthorized disclosure or production of national security information, other classified information and other nonclassified information in the files of the FBI;
>
> I understand that unauthorized disclosure of information in the files of the FBI or information I may acquire as an employee of the FBI could result in impairment of national security, place human life in jeopardy, or result in the denial of due process to a person or persons who are subjects of an FBI investigation, or prevent the FBI from effectively discharging its responsibilities. I understand the need for this secrecy agreement; therefore, as consideration for employment, I agree that I will never divulge, publish, or reveal either by word or conduct, or by other means disclose to any unauthorized recipient without official written authorization by the Director of the FBI or his delegate, any information from the investigatory files of the FBI or any information relating to material contained in the files, or disclose any information or produce any material acquired as a part of the performance of my official duties or because of my official status.
>
> That I understand unauthorized disclosure may be a violation of Federal law and prosecuted as a criminal offense.

9. On October 22, 1984, PITTS signed the Classified Information Nondisclosure Agreement, which reads in part:

> I have been advised and am aware that direct or indirect unauthorized disclosure unauthorized retention or negligent handling of classified information by me could cause irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge such information unless I have officially verified the recipient has been properly authorized by United States Government to receive it or I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) last granting me a security clearance that such disclosure is permitted. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.
>
> I have been advised and am aware that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; and the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised and am aware that any unauthorized disclosure of classified information by me may constitute a violation of United States criminal laws including the provisions of Sections 641, 793, 794, 798, and...the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982.

10. PITTS currently holds a "Top Secret" security clearance. From November 15, 1989 until November 18, 1996, PITTS held certain additional "code word" clearances for access to sensitive compartmented information.

11. Upon graduation from the FBI Academy, he was assigned to the FBI's Alexandria Field Office where he worked applicant, white collar crime and narcotics investigations. PITTS was assigned to the Fredericksburg Resident Agency within the Alexandria Field Office from March 18, 1985 through January 21, 1987.

12. PITTS was assigned to the New York Field Office from January 31, 1987 to August 13, 1989. He worked FCI investigations including investigations concerning KGB officials assigned to the (then) Soviet Mission to the United Nations.

13. In August 1989 PITTS was promoted to Supervisory Special Agent and transferred to the Document Classification Authority Affidavit Unit within the Operations Section of the Records Management Division at FBI Headquarters, in Washington, DC. Upon assignment to the Records Management Division, PITTS was granted access to Sensitive Compartmented Information. In 1991, he was reassigned to the Security Programs Section, where he was responsible for supervising personnel security investigations.

14. On or about October 18, 1992, PITTS was transferred to the Legal Counsel Division at FBI Headquarters, where he worked in DNA Legal Assistance and was then assigned to civil litigation matters. PITTS worked in FBI office space located within a building at 601 Pennsylvania Avenue, NW, Suite 750, Washington, DC.

15. On or about January 23, 1995, PITTS began working in the Behavioral Science Unit, FBI Academy in Quantico, Virginia, where he remains at present. Among his responsibilities at the FBI Academy is to conduct security briefings for FBI personnel.

16. Since PITTS' assignment to the FBI Academy, PITTS had no duty or responsibility that would have required or necessitated ongoing contact with Russian citizens in a foreign counterintelligence capacity. PITTS was not authorized in 1995 or 1996 to meet with agents of foreign counterintelligence services. In addition, PITTS was required by FBI policy and procedure to accurately and fully report such contacts, which he did not do.

17. This affidavit refers to information obtained from electronic surveillance, video surveillance and searches of various places and things. In each instance, the searches and surveillance described in this affidavit were authorized by court order, or by consensual monitoring.

Espionage-Related Activities (1987-1992)

18. In January, 1987, PITTS began his duties with the New York Division, assigned to a squad responsible for various FCI investigations. Between January, 1987 and August, 1989, PITTS had access to a wide range of sensitive and highly classified operations. These included the following: recruitment operations involving Russian intelligence officers, double agent operations, operations targeting Russian intelligence officers, true identities of human assets, operations against Russian illegals, true identities of defector sources, surveillance schedules of known meet sites, internal policies, documents, and procedures concerning surveillance of Russian intelligence officers, and the identification targeting and reporting on known and suspected KGB intelligence officers in the New York area.

19. In 1988, PITTS described his duties in New York as follows:

> my current duties in NY include investigations concerning Soviet intelligence officers, Soviet establishments, Soviet emigres, espionage matters and developing assets. These duties have afforded me an opportunity to investigate some highly complex and sensitive cases, including identification of Soviet intelligence officers, identifying Soviet efforts directed at the emigre community and participation in recruitment efforts.

The July 1987 Letter

20. In or about late July 1987, a cooperating witness (hereafter, "CW"), who is known to be reliable and credible, received a letter addressed to the CW at the (then) Soviet Mission to the United Nations. At the time, the CW was a citizen of the Soviet Union assigned

to the Soviet Mission to the United Nations. The letter provided surveillance information concerning the CW's recent activities.

21. Specifically, CW recalled that the letter received from the writer contained reference to a trip which CW had made to a New York City airport to meet two high-ranking KGB officials several days earlier. Review of FBI records indicates that on July 15, 1987—one week before it is believed the letter was sent to CW—PITTS conducted surveillance on the CW at another New York City airport and later reported the surveillance in a memorandum classified Secret.

22. Based on the foregoing, the CW concluded that the writer was an FBI employee. In the letter, the writer requested a meeting with the CW or, if the CW was not a KGB officer, with an actual KGB officer. (During the summer of 1987, several Special Agents on the counterintelligence squad to which PITTS was assigned, wrongly concluded the CW was a senior KGB officer. PITTS, himself, told the CW in December, 1995, that he had chosen the CW to meet with because the CW had been "misidentified" [as a KGB officer].)

23. The CW provided the letter to the Mission Security Officer, Vadim Voytenko (hereafter, "Voytenko"). Later, the CW met with Voytenko and Aleksandr Vasilyevich Karpov (hereafter, "Karpov").

24. Based upon investigation and analysis, Aleksandr Vasilyevich Karpov has been identified by the FBI as an officer of the SVRR and, formerly the KGB. From 1987 through 1990, he was the New York Chief of Line KR. Line KR, the counterintelligence component of the KGB, was responsible for penetrating the intelligence and security services of foreign nations, including those of the United States, by human and technical means. The FBI was one of the intelligence/security services targeted by Line KR.

The Meeting at the New York Public Library

25. The CW was instructed by Voytenko to meet with the writer of the letter at the New York Public Library, located at Fifth Avenue and 42nd Street in New York City. The CW briefly met the writer inside the library, and then introduced the writer to Karpov.

26. Based upon statements made by PITTS during the "false flag" operation, information provided by the CW, and based upon PITTS' subsequent conduct and on other investigative activities, I believe that the writer of the letter to the CW was PITTS and that PITTS was the U.S. intelligence officer who met with the CW and Karpov at the New York Public Library.

Disclosure of Classified Material

27. The meeting between Karpov and PITTS at the New York Public Library was the beginning of five years of active espionage activity by PITTS on behalf of the KGB and SVRR.

28. I believe that among the classified documents and information which PITTS conveyed to the KGB in the course of his espionage activity in return for money were the following:

a. A document known as the "Soviet Administrative List." The "Soviet Administrative List" was the FBI's computerized, alphabetical compilation of all Soviet officials posted or assigned to the United States. It is classified "Secret" and is related to the national defense. The "Secret" classification is applied to information whose unauthorized disclosure reasonably could be expected to cause serious damage to the national security. The list contains the names, dates of birth, posting, in-country/travel/out-country status, file number, FBI office of origin, FBI squad, FBI case agent, and the known or suspected intelligence affiliation of each Soviet official assigned to Soviet legations in the United States, including the Soviet Embassy in Washington, D.C., and the Soviet Mission to the United Nations in New York, New York.

PITTS was not authorized to deliver the "Soviet Administrative List" to any person not employed by the FBI nor to any person within the FBI who did not have an official need to know the information contained in the list.

b. A letter to CW, then suspected by the FBI of being a KGB officer, containing surveillance information concerning CW. Specifically, PITTS disclosed classified Secret information concerning FBI surveillance of CW.

c. Secret information concerning an FBI asset who reported covertly on Russian intelligence matters.

Information Obtained in the "False Flag" Operation Concerning PITTS' 1987-1992 Espionage Activity

29. The FBI conducted an analysis of PITTS' financial affairs and travel records and conducted additional investigation, including the debriefing of CW by the FBI. In or about August 1995, a "false flag" operation was initiated. A "false flag" operation is an operation intended to persuade a target of the operation that he is working for one country when, in fact, he is working for another. The purpose of this "false flag" operation was to confirm PITTS' 1987-1992 suspected espionage activities and, most importantly, to determine what FBI information, projects and operations PITTS had compromised by divulging them to the KGB and SVRR during the course of his espionage activities.

30. Specifically the "false flag" operation was designed to persuade PITTS through the use of the CW, and through the use of U.S. government personnel posing as SVRR officers, that he was being contacted again by the SVRR and then, in the course of conducting current espionage-type activites, ascertain the scope and content of his past espionage activities. In fact, during the course of the "false flag" operation, PITTS made numerous incriminating statements concerning his prior espionage activites, including the following:

a. On or about September 8, 1995, PITTS wrote a letter to the person he believed to be his new SVRR handler in which he apologized for missing a meeting with his old SVRR handler in New York and stated that he was "very pleased to hear from you again."

b. In the same September 8, 1995 letter described above, PITTS indicated that he did not have information concerning a certain KGB official and stated: "Shortly after I last met with Alex, I left the operational side of the business and became more of an administrator and researcher." The reference to "Alex" is believed to be a reference to one of PITTS handlers, Aleksandr Karpov.

c. In the same September 8, 1995 letter described above, PITTS stated: "I have no additional material to pass along as collections ceased when I missed your friend in New York."

d. On or about November 2, 1995, PITTS wrote a letter to the person he believed to be his SVRR handler. In this letter, PITTS made reference to "previous exchanges." (This letter was not in fact sent due to PITTS' discovery of a surveillance device.)

e. In the same November 2, 1995 letter, PITTS asked for $35,000 to $40,000 from "my account" to fund an escape plan. It is believed that this reference to "my account" is a reference to an account set up in Russia on PITTS" behalf.

f. On December 17, 1995, a telephone call took place between PITTS and the person he believed to be his SVRR handler. In that call, the "SVRR [FBI]" handler told PITTS that PITTS needed to have a face-to-face meeting with PITTS' friend from Moscow. The "SVRR [FBI]" handler told PITTS that "you must come to the place where you first requested to meet in 1987." PITTS acknowledged that he remembered the place [the New York Public Library] and the section in the place where the 1987 meeting had occurred.

g. On December 28, 1995, a telephone call took place between PITTS and the person he believed to be his SVRR handler. The call concerned the fact that the meeting scheduled for earlier that day in New York had not taken place as planned. After the "SVRR [FBI]" handler told PITTS that his friend had been waiting in one section of the library for PITTS, PITTS stated that this section was "not where we first met" and that their first meeting had been in a different section of the library. I believe this is a reference to PITTS' first meeting with the CW in or about July, 1987.

h. In a December 29, 1995 meeting with a person he believed to be his SVRR handler, PITTS was asked if he had brought anything for the handler. PITTS said he had not because "before" we were "never supposed to exchange two things." I believe this is a reference to the procedures PITTS used during his espionage activity between 1987 and 1992.

i. In the same December 29, 1995 meeting, PITTS said: "I feel very uneasy compared to last time, it's, uh, I'm much more out of out of touch with what's going on." I believe this is a reference to PITTS' espionage activity between 1987 and 1992.

j. In the same December 29, 1995 meeting, the following exchange took place between an Undercover officer ["UCO"], who was posing as an SVRR officer, and PITTS:

UCO: Edwin, does your wife know anything about our present project?

PITTS: No, No. She doesn't know about any of the Projects but she....

UCO: Did she know anything about the project when you worked with Alex in the old days in New York?

PITTS: No, unless she suspected. She has great deals of suspicions.

UCO: You had no problem with that then in New York at the time?

PITTS: No.

k. In the same December 29, 1995 meeting, the following exchange took place:

UCO: Do you remember the last date when you met Alex [Karpov]?

PITTS: No.

UCO: You don't? The year?

PITTS: Oh, the year? The year would have been, um, uh, 1988.

l. In the same December 29, 1995 meeting, the following exchange took place:

UCO: . . . the money you got in the past . . . there was some doubt that you perhaps did not get all the money which was coming to you, to your account.

PITTS: No, I didn't. No . . . but,

UCO: No. You . . .

PITTS: But, I mean, I understand, we had to break contact.

UCO: Yeah, but I understand those people who did bring you money at the time or that money which was passed to you . . .

PITTS: Um Hum.

UCO: They, well, tried to reach us, establish to see if your account is up to date. We have an account, you know this?

PITTS: Um Hum. Yes.

UCO: Are you aware of the account?

PITTS: Well, Yeah, I've been told about it.

UCO: Yeah, did ever mention how much it is, in the account?

PITTS: Alex did, but I, I don't remember the amount.

UCO: You don't remember?

PITTS: No. I've tried to put those things out of my head.

m. On July 9, 1986, PITTS wrote a letter to the person he believed to be his SVRR handler, which reads in part:

If it is possible, please make payment for my most recent deliveries (or withdraw from my reserve account) . . .

n. On or about August 14, 1996, PITTS wrote a letter to the person he believed to be his SVRR handler, which reads in part:

Regarding my reserve, I do not know the amount and it is my understanding that you do not. When I last met with Alex, it was over 100,000.

o. In the same August 14, 1996 letter, PITTS stated that it might be appropriate for the SVRR to pay him out of his "reserves" because "much of the information I have recently provided is not of the quality I have provided in the past . . . ."

p. On or about September 18, 1996, PITTS made additional statements in a letter to the person he believed to be his SVRR handler concerning moneys he had received in the course of his espionage activities during the 1987 to 1992 time period. In this excerpt, PITTS made reference to an SVRR officer who handled PITTS after Alexander Karpov:

> During the time I knew him, two payments were made but I can not remember if they were in round numbers. He never spoke of the size of the reserve fund or how much I was to expect in payment. The greatest difficulty was the distance between our locations and the absence of an alternate means of communicating meeting dates and alternate dates. The distance and time between meetings made it impossible to plan for unforeseen circumstances. The nature of the information changed because of the type of work I was assigned. I only met him two, or maybe three, times after my posting to Washington (in 1989).

q. On December 13, 1996, in a communication to the persons he believed to be his SVRR handlers, PITTS stated that he no longer had "direct access" to the files from his New York assignment (1987-1989) but "I believe I have provided you with everything that I was aware of."

r. In the same December 13, 1996 communication, PITTS stated that he wished "to draw on reserve funds" on January 6, 1991 and February 6, 1997. I believe this to be a reference to the Russian account set up on behalf of PITTS, as described, above.

Trips to New York City in 1990-1992

31. In August 1989, PITTS was transferred from the New York Field Office of the FBI to FBI Headquarters. Beginning in February 1990, and continuing to October 1992, PITTS made a series of nine brief trips to New York City, most of which were one day trips, all such trips taken to or from National Airport, in the Eastern District of Virginia. Financial analysis indicates a pattern of unusual monetary deposits following these trips. I believe that PITTS made all or most of these trips for the purpose of continuing his espionage activities.

Financial Analysis

32. The FBI has conducted a financial analysis of PITTS for the time period in which it is believed PITTS was actively involved in espionage activities on behalf of the KGB and SVRR. This financial analysis indicates that PITTS acquired substantial money during this period of time which cannot be traced to legitimate sources of funds.

33. PITTS' only known source of substantial income during the period from 1987 to 1992 was from his employment and his wife's employment with the FBI. PITTS made frequent deposits of cash and/or money accounts or as payments on credit card accounts. This activity was unusual as compared to PITTS' normal financial banking activity prior to July, 1987 and subsequent to June, 1992. Furthermore, examination of when money orders were purchased and when groupings of deposits were made, revealed a pattern linking such deposits to the dates of PITTS' New York trips.

34. From 1987 to 1992, these unexplained deposits and credit card payments resulted in an enhancement of PITTS' wealth by over one hundred thousand dollars, as follows:

YEAR	TOTAL VALUE OF DEPOSITS
1987	$2,775.00
1988	5,024.48
1989	23,414.31
1990	35,520.00
1991	29,115.21
1992	28,375.66
TOTAL	**$124,224.66**

This sum of money does not include any funds PITTS may have received which were not deposited into one of his accounts or used to pay bills. Nor does it include the account in Russia which, according to PITTS' statement, was funded with "over $100,000."

35. PITTS utilized a number of financial institutions and accounts to hide his receipt of this unexplained wealth, including several accounts at financial institutions in the Eastern District of Virginia. The deposits to these accounts were small, no larger than

$1,100.00, and spread out over several days within a month. To further conceal the receipt of illegal funds, PITTS rented a post office box in Washington, D.C., which received the American Security Bank statements, he made innumerable deposits, withdrawals, and transfers via automated teller machines, and he purchased multiple money orders for deposits into his bank accounts and for payments on credit and accounts. For example, in the years 1987-1992, over 50 money orders were purchased by PITTS.

36. The following is a summary of activity concerning the specific accounts listed above that have led me to believe these accounts contain proceeds of PITTS' espionage activity:

a. Name/Company: PENTAGON FEDERAL CREDIT UNION
Address: Alexandria, Virginia
Account #: 587571-027
In name of: EARL EDWIN PITTS and Mary Colombara Pitts
Activity: From July 1987 through May 1992, there were thirty-five known deposits to this account totaling, approximately $10,595, all unexplained by PITTS' known income.

Account #: 587571 019
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From September 1987 through April 1992, there were thirty-two known deposits to this account totaling approximately $8,419, all unexplained by PITTS known income.

b. Name/Company: CENTRAL FIDELITY BANK
Address: Richmond, Virginia
Account #: 1018713721
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From July 1989 through July 1992, there were twelve known deposits to this account totaling approximately $4,591, all unexplained by PITTS' known income.

Account #: 7919862232
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From July 1989 through October 1992, there were one hundred fifty one known deposits to this account totalling approximately $38,612, all unexplained by PITTS known income.

Name/Company: KEY OF NEW YORK
Address: Albany, New York
Account: 342928376
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From June 1988 through August 1989, there were fifty-three known deposits to this account totalling approximately $10, 488 all unexplained by PITTS known incomes.

Account #: 347009151
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From September 1988 through June 1989, there were nineteen known deposits to this account totalling approximately $1,354, all unexplained by PITTS' known income.

d. Name/Company: CHEMICAL BANK (MANUFACTURERS HANOVER)
Address: New York, New York
Account #: 0630264
In name of: EARL EDWIN PITTS and Mary Colombaro Pitts
Activity: From January 1989 through August 1989, there were thirty-two known deposits to this account totaling approximately $8,027, all unexplained by PITTS'known income.

e. Name/Company: NATIONS BANK (AMERICAN SECURITY)
Address: Baltimore, Maryland
Account #: 11661881

In name of: EARL EDWIN PITTS
Activity: From March 1990 through August 1992, there were one-hundred twenty known deposits to this account totaling approximately $33,735, all unexplained by PITTS' known income

Espionage–Related Activities (1995-1996)

37. In August 1995, the FBI initiated the "false flag" operation described above. It began with correspondence, postmarked in New York, New York, and sent to PITTS' residence. There was no response.

The August 26, 1995 Meeting

38. On or about August 26, 1995, at approximately 2:30 p.m., the CW went to the PITTS residence and met PITTS at the door. He told PITTS:

> There is a guest visiting me. He wanted to see you. He's in my car. He's from Moscow.

39. PITTS agreed to meet with the CW and the "guest from Moscow" one hour later at the Chancellorsville Battlefield Visitor Center.

40. At approximately 3:20 p.m. that same day, PITTS met the "guest from Moscow," an undercover intelligence officer (hereafter, "UCO"), at the Chancellorsville Battlefield Visitor Center.

41. The UCO told PITTS that the reason he was there was to advise him of a mutual problem. The UCO indicated that the "SVRR" was worried about the behavior of a Resident [a senior SVRR official] who had been recently assigned in the United States and requested PITTS' assistance.

The UCO asked PITTS:

> UCO: Have you brought anything for me, with you? Anything you can give me? Maybe you have some.
>
> PITTS: I, I have nothing. I wasn't expecting you.

42. The UCO stated that his superiors were very happy with PITTS and highly appreciative of PITTS' help and asked if PITTS would help them. PITTS responded: "I'll help you if I can." PITTS added that he was in "another line now," and did not have good access.

43. The UCO provided a sealed envelope to PITTS which contained written instructions to PITTS describing how PITTS should make a "dead drop" at a particular location code-named "POLE" on September 9, 1995 in the Clifton, Virginia area. (A "dead drop" is a prearranged location where a clandestine foreign agent or intelligence officer may utilize impersonal, clandestine means of communication to transfer tangible objects between them.) PITTS was also instructed to mark a signal site, codenamed "GRADE," in this same area once the "dead drop" had been put down. Also included in the envelope was "SVRR [FBI]" tasking for PITTS to accomplish and provide in the future.

44. The UCO asked PITTS about his financial situation and indicated that money was available if PITTS needed it. PITTS responded by asking if the UCO had the money with him. The UCO told PITTS that he did have the money with him and PITTS stated that he "could" use the money. The UCO gave PITTS a sealed envelope containing $15,000.00 in used, unmarked, non-sequential, $100 bills. PITTS placed the envelopes in his pants' pocket.

45. The meeting ended with PITTS stating, "I'll do what I can."

Mary Pitts' Suspicions

46. On August 26, 1995, the day of the first "false flag" contact, Mary Pitts talked to her sister on three occasions. She said that on that day a man with a foreign accent came to the house and asked for PITTS, after which PITTS left the house in a "panic." Mary Pitts warned that she didn't want to talk about it over the phone, but she confronted PITTS with what she found. (She searched PITTS' home office while he was meeting with the "SVRR [FBI]".) Her sister then asked if that included "the secret stuff" and Mary Pitts answered affirmatively.

47. On or about August 29, 1995, at approximately 8:00 a.m., Mary Pitts telephoned Special Agent Tom Carter at the Fredericksburg Resident Agency, and asked him to meet with her on an urgent and confidential matter

concerning her husband. Special Agent Carter met with Mary Pitts for approximately an hour and obtained statements from her regarding PITTS' suspicious activities on August 26, 1995 and a copy of the initial "false flag" letter referred to above. Special Agent Carter advised Mary Pitts that he would look into the matter for her, and that he would get back to her as soon as possible.

48. Later that day, Mary Pitts had a telephone conversation with a neighbor in which she expressed concerns about PITTS' conduct and her own decision to report her husband to the FBI:

Mary: I probably shouldn't gone to the Bureau and it will probably be the end of my marriage either way it goes because if he find . . . If he is on the up and up and he finds out that I went behind his back we're finished.

Neighbor: Ahm, the thing of it is Mary. You did what you had to do at the time and there is no point in beating yourself.

Mary: There is no going, there is no going back now . . .

Neighbor: No, no beating yourself over that…

Mary: What price for national security.

Neighbor: Were you worrying about national security really?

Mary: Yeah, part of me is.

Neighbor: Yes.

Mary: Because, you know I have… There is things wrong with this country but it's still my country.

Neighbor: Yeah.

Mary: And passing information to a foreign national or a foreigner, a foreign country…

Neighbor: Well if it turns out to be the case then you know you did the right thing. You did the only thing.

Mary: Even though maybe he would have stopped in a, in a while? What you would have stopped at my request and we could have gone on with our wonderful life?

Neighbor: Don't know, uh see…

Mary: Could I have gone on with my regular and wonderful life? It's over, my life is over.

Events of August 29, 1995– August 30, 1995

49. At approximately 9:00 a.m., on or about August 29, 1995, while sitting in his office, PITTS took from his gym bag, under his desk, an envelope believed to contain the operational instructions given to him by the UCO on August 26, 1995. PITTS read the instructions, consulted his calendar, and returned them to the envelope, which he put in his desk drawer.

50. At approximately 1:00 p.m., on or about August 29, 1995, PITTS took an envelope of money from his gym bag under his desk and proceeded to count and separate the money into stacks of ten bills. PITTS placed each stack into a white letter size envelope, 15 envelopes in all. PITTS sealed each envelope and placed the envelopes into one large manila envelope, along with what appeared to be the written instructions for the "dead drop" site, and placed the large envelope into his desk drawer.

51. At approximately 8:00 a.m., on or about August 30, 1995, PITTS concealed a large manila envelope in a ceiling panel of his office. The envelope contained the money and instructions previously furnished to PITTS by the UCO on August 26, 1995.

PITTS' Meeting with Agent Carter

52. After learning from his wife that she had talked to Special Agent Carter about her suspicions, PITTS asked for a meeting with Special Agent Carter. At approximately 10:52 a.m., on or about August 30, 1995, PITTS meet with Special Agent Carter in PITTS' office space. PITTS was calm and made a series of statements to Special Agent Carter to explain the situation which transpired between himself and his wife on August 26, 1995, as follows: A man visited their home on August 26, 1995, who PITTS explained was an asset he knew while working in the New York Division. The name provided by PITTS to Special Agent Carter was the

name of a person other than the CW. Due to their previous relationship and the fact that PITTS was a lawyer, the asset sent PITTS a note asking him to come to New York. Because of the asset's drunken state when the asset appeared at PITTS' residence, PITTS met the asset at the Walmart near his home to render legal advice. These statements were false.

53. At approximately 4:30 p.m., on August 31, 1995, in PITTS' office, PITTS took a white letter-sized envelope out of his filing cabinet and opened it. He took from the envelope ten bills and proceeded to examine each bill by placing them up against the light. PITTS returned nine of the bills to the envelope and placed the envelope back in his filing cabinet. He placed one bill into his wallet.

Office Search on August 31, 1995

54. A search was conducted on August 31, 1995 of PITTS' office space at the FBI Academy, Quantico. The search revealed the following: a legal size manila envelope found inside a five drawer filing cabinet, located behind PITTS' desk, which contained 15 sealed white, letter-sized envelopes, and one manila, letter-sized envelope that was folded but not sealed. The manila envelope contained the written "dead drop" instructions provided to PITTS by the UCO on August 1995. Each one of the 15 white envelopes were sealed and contained money in what appeared to be denominations of $100.00. The serial number of one bill in each envelope, which could be seen through the envelopes, matched those provided to PITTS by the UCO on August 26, 1995.

Events of September 7–8, 1995

55. At approximately 8:33 a.m., on September 7, 1995, PITTS retrieved the "dead drop" instructions furnished to him by the UCO on August 26, 1995 from his hardcover briefcase. He placed the instruction in plastic pockets of a dark colored binder, and discarded the envelope from which they came.

56. At approximately 11:49 a.m., on the same day PITTS took a large manila envelope from his legal attaché case. PITTS took a smaller, white envelope out of the manila envelope and withdrew cash from it, afterwards marking on the white envelope. PITTS placed the cash in a pre-addressed, small, white envelope. He also took money from his money clip and placed this into the pre-addressed envelope as well. PITTS then placed the pre-addressed envelope and the money envelopes into a stenotype folder on top of his desk.

57. On or about September 8, 1995, PITTS arrived at his work place at approximately 7:18 a.m. At approximately 7:29 a.m., PITTS began typing on his laptop computer.

58. At approximately 7:38 a.m., PITTS took out a Northern Virginia map and the "dead drop" instructions which were stored in a dark colored binder. PITTS studied both the map and the instructions, then placed the binder into his bottom, right desk drawer.

59. At approximately 10:43 a.m., PITTS put on a pair of gloves. PITTS then retrieved a 3.5" computer disk, wiped the disk off with the gloves and placed it into the hard drive of his laptop computer and began typing. At approximately 10:32 a.m., PITTS looked at the dead drop instructions contained in the dark colored binder. PITTS continued to glance at the instructions intermittently while typing. At approximately 10:46 a.m., PITTS took out a small piece of paper and briefly wrote on it, while wearing gloves. At approximately 12:37 p.m., PITTS took the disk out of his laptop hard drive and replace it with another one. One minute later, PITTS exchanged the disks again, replacing the new one with the original. At approximately 12:39 p.m., PITTS took a map out and looked at it. At approximately 12:40 p.m., he took a plastic bag from his briefcase, and placed one disk into the plastic bag. This disk was placed into his briefcase, while another disk was placed into a disk storage container, taped shut, then placed in a file cabinet. At approximately 12:44 p.m., PITTS reviewed a map and then the dead drop instructions in the binder. PITTS departed his office at approximately 12:53 p.m.

60. PITTS entered the Clifton, Virginia, area at approximately 2:11 p.m. PITTS proceeded directly to the "dead drop" location in Clifton, arriving at the "dead drop" site at approximately 2:30 p.m. PITTS placed a package containing a 3.5" computer disk into the "dead drop." The disk was wrapped in a plastic sandwich bag, which was then concealed in a paper bag.

61. PITTS proceeded to signal site "Grade," and at approximately 2:40 p.m. marked the signal site as previously instructed. PITTS departed the Clifton area at approximately 3:10 p.m. and proceeded back to his work place.

62. The package retrieved from dead drop "Pole" contained a note with the signature, "Edwin Pearl" [a code name for PITTS] and a computer disk which contained a file named "Alex" which, in part, said:

> I was very pleased to hear from you again. I'm sorry I missed your friend when I was in New York. I discovered I had gone to the wrong location and by the time I realized my mistake I missed the get together. Unfortunately, I did not have ready access to a telephone number or address where I could contact you and could not invite you or your friends to any future get togethers.

It is my belief that PITTS was referring to a missed meeting with his SVRR handler in New York.

63. The file also contained the following statement by PITTS:

> I appreciate your concern for my well being, but there should be no great concern on your part. It appears to me that there are several aspects about our system that are greatly different from your concept of our system. It is possible to insulate one's self from real harm even if all security systems fail. There are certain legal and political factors one can rely on to prevent a serious threat to one's safety. Therefore, I strongly recommend you take no dramatic action on my behalf, even if you have had a total problem within your system. My sudden movement would only confirm suspicions if they exist and could seriously harm the degree of cordiality that is being developed between our principals. If I am confronted, I can use certain procedures to protect myself from any long term harm.

Office Search on September 13, 1995

64. On September 13, 1995, a search was conducted at PITTS' office space at Quantico. The search revealed the following: a dark colored binder was located in PITTS' file cabinet which contained the "dead drop" instruction note furnished to PITTS by the UCO on August 26, 1995. A sheet of paper containing the alias signature "Edwin Pearl" was also located in the binder.

October 18, 1995 Drop by "SVRR [FBI]" and Pick Up by PITTS

65. At approximately 5:12 a.m., on October 18, 1995, the FBI posing as the "SVRR," placed a 3.5" computer disk, wrapped in plastic, at the appointed drop site in Fairfax County, Virginia. The disk contained tasking for PITTS and operational planning for future-drop activities.

66. PITTS left his residence at approximately 8:00 a.m. He drove to his work place and entered his office at approximately 8:45 a.m. He took a dark colored binder from his file cabinet and several envelopes, and then left his office at 9:60 a.m. During the next two hours, PITTS drove to various locations in what I believe to be an effort to detect surveillance.

67. Technical coverage at the drop site revealed that PITTS arrived from a westerly direction on Yates Ford Road, at approximately 11:21 a.m. He left the drop site at approximately 11:27 a.m. and left the area, heading north on Highway 123 to the signal site. Instead of turning right at Burke Center Parkway, as would be the most direct route, PITTS continued north on Highway 123, .25 miles north of Burke Center Parkway. He turned left into Fairfax Station Square Shopping Center at approximately 11:46 a.m. PITTS exited his vehicle and walked toward one of the stores. PITTS was next seen in a southbound direction on Highway 123, turning left onto Burke Center Parkway. He turned left into Burke Center Shopping Center and parked in the western end of the parking lot. He entered CVS Pharmacy, exited and walked toward Baskin Robbins. He entered Baskin Robbins, bought an ice cream cone and stayed in the store for approximately ten minutes. He exited the store, looked around the area, walked across the street and marked the signal on a fire hydrant as he passed by. He then walked through the parking lot back toward his vehicle. Before reaching his vehicle he returned (through the parking lot) to the area of the signal site. He once again looked around, looked at the signal site from across the street (in front of Baskin Robbins), then walked down the sidewalk and back to his vehicle, leaving the shopping center at approximately 12:03 p.m.

Events of November 1, 1995–November 3, 1995

68. On or about November 1, 1995, PITTS was observed typing on a laptop computer in his office, looking through and writing in spiral notebooks, looking at a dark colored binder and handling and reviewing documents marked "Secret." These activities collectively lasted approximately 176 minutes.

69. On or about November 2, 1995, PITTS spent approximately 95 minutes typing on his laptop computer in his office at work.

70. On or about November 2, 1995 at approximately 8:26 p.m., a search of PITTS' office revealed the following items of interest: a handwritten note with names of FBI Special Agents recently transferred to the National Security Division at FBI Headquarters; a handwritten note describing a Northern Virginia Public storage facility at 7400 Alban Station Boulevard, with telephone number (703) 569-6926; a 3.51" computer disk labeled "PITTS" which contained the information passed via "dead drop" on September 8, 1995; and a dark colored binder containing, in part, "dead drop" and signal site locations and a photocopy of the note with the name "EDWIN PEARL" on it.

71. During the same search on November 2, 1995, the hard drive on PITTS' personal notebook computer was searched. It contained a six page, single spaced, letter to PITTS' "SVRR handlers."

This letter included the following:

Information concerning past and current FCI operations in New York, Los Angeles and Washington, D.C., identifying information concerning eight FBI agents, including himself, including such information as home address, current assignment, and number of children. (PITTS made reference to himself in this letter in the third person, as if the letter had been composed by someone else.)

Information concerning an "emergency escape plan in the event it needs to be used on short notice."

Information concerning PITTS' plan to provide and receive information via a computer disk left in a storage facility in the Springfield, Virginia, area.

72. I believe that PITTS was preparing this document to pass via computer disk to persons he believed to be the SVRR on the scheduled drop dates of either November 1, November 2, or November 3, 1995. (This document was not in fact passed due to the discovery by PITTS of a surveillance device.)

73. On November 3, 1995, it was determined that PITTS had discarded the following, among other items:

1) ten typewritten pages with classified markings cut off;

2) ten pieces of paper stamped "Secret" which appeared to be from the cut off tops of a document;

3) ten pieces of paper stamped "Secret" which appeared to be cut off from the bottom portion of a document.

November 16, 1995 Telephone Contact

74. On or about November 16, 1995, PITTS was telephonically contacted by an undercover FBI Special Agent (hereinafter "UCA") posing as an SVRR officer. PITTS received the call at a public telephone near the FasMart Convenience Store, located at the intersection of Kilarney Drive and Route 3, Fredericksburg, Virginia.

75. During the telephone conversation, the UCA instructed PITTS to retrieve two keys and a slip of paper from a magnetic box located underneath the telephone. PITTS was told the keys were for a mailbox and the address of the mailbox was on the paper. The keys open Box 318, located at a Mailboxes Etc., facility in the Eastern District of Virginia, hereafter referred to as "Box 318."

November 17, 1995 Drop

76. On or about November 17, 1995, PITTS placed a computer disk in Box 318. This disk contained a letter to the person PITTS believed to be his SVRR handler. The letter included the following: apologies for missing the last meeting, information regarding the discovery and arrest of Aldrich Ames, and the risks associated with exchanging information via a mailbox.

77. On or about November 17, 1995, PITTS was paid $10,000.00 by what he believed to be the SVRR via Box 318.

December 13, 1995 Drop

78. On or about December 13, 1995, PITTS delivered a computer disk via Box 318. This disk contained a letter to the person PITTS believed to be his SVRR handler. The letter included the following: information regarding technical penetrations in use by the FBI, his use of surveillance detection routes, and the identities of FBI agents who had access to operations conducted against the KGB while PITTS was assigned to the New York office and their current assignments.

Events of December 17, 1995, December 28, 1995 and December 29, 1995

79. On December 17, 1995, PITTS had a telephone conversation with the person he believed to be his SVRR handler. In fact, the person posing as an SVRR officer was an FBI Undercover Agent (hereafter, "UCA"). In the conversation, the UCA and PITTS set up a meet. Significantly, PITTS was never told precisely where the meet was to take place; rather, he was told to meet at the same location where he had first met the CW in 1987 (i.e., the New York Public Library]:

UCA: Okay. Edwin. Thank you for your package and your signal was received and ah, ah, listen Edwin. Ah, your friend from Moscow has come and he must speak to you face-to-face to discuss some important matters and give you something substantial from your account and a Christmas bonus also, okay?

PITTS: Okay.

UCA: Okay. Now, Edwin. Ah, you must come to the place where you first requested to meet in 1987. Do you remember this place?

PITTS: Ah, yes.

UCA: Okay, good. Now you remember the section where you came?

PITTS: Ah, I believe so. Yes.

UCA: Good. Good. Okay, Edwin. We will meet you there, okay?

PITTS: Okay.

UCA: Go to the same place you first requested to meet and arrive there at thirteen hundred hours. One three zero zero.

PITTS: Okay.

UCA: At the same table, in the same section at this place.

PITTS: Okay.

UCA: And you will see somebody, someone you already know. Somebody already known to you. Okay?

PITTS: Okay.

UCA: This person will give you instructions.

PITTS: Okay.

The meet was set for December 28, 1995 at 1 p.m.

80. The meet described above did not take place. PITTS traveled to New York City and followed a surveillance detection route provided to him by his "SVRR [FBI]" handler. He then went to the New York City Public Library and spent approximately 30 minutes in several rooms of the library. PITTS then left the library and returned to Virginia.

81. At 5:35 p.m., on December 28, 1995, PITTS and the undercover agent spoke on the telephone:

UCA: Edwin, what happened?

PITTS: Uh, I was there in the room. I, I, none of your friends were there.

UCA: Okay. Now, uh, a friend that you know, a person whom you know waited for you and was seated at the table in the Law Section of Room 228, and waiting for you.

PITTS: Okay. That's not where we first met.

UCA: It is not where you met?

PITTS: No.

UCA: Oh, where did you meet? You know I, I thought that this is the place that you met. Where did you meet him the first time?

PITTS: No, it was in the uh, uh, I think it is called the Public Affairs and Economics.

UCA: Public Affairs and Economics you think that is where you met him?

PITTS: Yes.

UCA: Because my people thought that you met him in the Law Section, in Room 228.

PITTS: No, it, it was around the corner. I, I thought there might be some confusion. I looked around uh, but I couldn't find him anywhere, I, I must have missed him in that section.

A second meeting was scheduled for the next day at National Airport. PITTS stated that he would do "everything I can" to make the meet and would "treat it importantly" but that he did not have "complete control" over his schedule. PITTS was told that the meet would be with "somebody that you know uh, somebody that knows you…."

82. On December 29, 1995, at approximately 10 a.m., PITTS arrived at National Airport and met with CW (the person to whom PITTS had written the 1987 letter):

PITTS: Hi. I'm sorry I, didn't, uh, like yesterday I couldn't find you inside the . . .

CW: You couldn't find the place, yes?

CW: I mean uh, you didn't remember the place, yes? Actually I went to this, the, the library where you took me for the first time after how many years have passed? (laughs)

PITTS: Well, I'm trying to remember.

CW: (laughs)

PITTS: Yeah, we met down on the, on the second floor . . .

CW: . . . how much time did you wait?

PITTS: No, I looked through the (word or two unclear) half an hour or so.

CW: And uh . . .

PITTS: I looked through the library, and I looked through other areas, but uh . . .

CW: But it was changed, you know? Because . . .

PITTS: Yeah.

CW: . . .when you invited me, then those computers were not in.

PITTS: Yeah, that's, that's what caused the confusion, really, the library had changed considerably, and it's full of computers now.

CW: Uh-huh, uh-huh! Well, I didn't say Merry Christmas, sir!

PITTS: Yes, also Merry Christmas to you.

CW: I have one funny question to ask you.

PITTS: Yes?

CW: Why did you select me? (laughs) You had that whole bunch of people in the, in the Embassy.

PITTS: Ah, it's because you were ah, you were misidentified [as a KGB officer].

83. CW then took PITTS to a parked car, where PITTS met with the undercover officer (hereafter, "UCO") posing as an SVRR official from Moscow. The UCO tasked PITTS, on behalf of the "SVRR [FBI]," to obtain a list of all our [SVRR] people from our services . . . who is known to your [FBI] people. By name and their avocation, what they really deal with. When asked if he understood the tasking, PITTS responded, "You, you, want a list of uh, of people with their, their overt cover and, and what we have them classified as." PITTS

was told that "should you provide this list to us, we are willing to pay you fifteen thousand dollars for this list."

84. On or about December 29, 1995, PITTS accepted $20,000.00 in payment for services from what he believed to be the "SVRR." The money was passed to PITTS by his "SVRR [FBI]" handler in a meeting which took place in a vehicle parked at National Airport, in the Eastern District of Virginia.

February 13, 1996 Drop

85. On or about January 29 and January 30, 1996, PITTS made arrangements with a pager company to buy a pager, which he picked up on or about February 1, 1996. PITTS purchased this pager to use for covert communication with what he believed to be his "SVRR" handlers. A paging system was established so the need to physically mark a signal site was eliminated and intentions to make a drop or a telephone call could be relayed via the pager. PITTS purchased this pager in furtherance of his espionage activities while using the pager issued to him by the FBI for other purposes.

86. On or about February 13, 1996, PITTS deposited a manila envelope in Box 318. The envelope contained an FBI document entitled: "Russian Administrative List," dated 10/20/95 consisting of 91 pages (pages 71 through 91 were repeated). The "Russian Administrative List" was marked "Secret" at the top and bottom of each page. In my opinion, this document is related to the national defense as that term is used in Title 18, United States Code, Section 794. This list was made available to PITTS in early November 1995 in the course of PITTS' regular duties at the FBI. While PITTS came into possession the "Russian Administrative List" in a lawful manner, he had no authority to duplicate the list for the purpose of conveying it to persons he did not believe to be authorized recipients.

87. On or about March 21, 1996, PITTS paged the "SVRR [FBI]" to his cellular phone and reported that he was not able to make his drop as planned, but would do so on the first, second or third of April. The following was part of this conversation:

> PITTS: Uh, yes, everything is fine uh, I'm making some progress on your request uh some of the things are more difficult than I thought but I have several avenues to explore so . . .
>
> UCA: Yes.
>
> PITTS: Ah I'll explain that in more detail uh when uh you get my package.

April 3, 1996 Drop

88. On or about April 3, 1996, PITTS placed an envelope in Box 318. The envelope contained a computer disk which contained a letter to the person he believed to be his SVRR handler. The letter included the following: information regarding numerous FBI Special Agents who had recently been given transfer orders to various FBI Field offices and Headquarters, a description of various FBI units within the National Security Division, and the names of FBI or other agency personnel who he said were assigned to national security related investigations.

89. In the same April 3, 1996 letter, PITTS promised his "SVRR [FBI]" handler that he would "attempt to gain an inroad" into a unit responsible for reviewing sensitive national security operations.

April 16, 1996 Drop

90. On or about April 16, 1996, PITTS placed an envelope in Box 318. The envelope contained three hundred fifty two pages. Included in the envelope were FBI telephone directories from The FBI Training Academy, FBI Headquarters, the Washington Metropolitan Field Office, FBI Field offices throughout the United States and FBI Legal Attaché Offices throughout the world. The envelope also contained FBI organizational charts from FBI Headquarters.

91. Such telephone directories including the FBI Headquarters directory referred to above, often contained on their front cover the following warning prohibiting unauthorized dissemination:

> This document is for internal use within the FBI, is to be provided appropriate security, and disposed of in official trash receptacles when no longer current.

April 24, 1996 Telephone Conversation

92. On or about April 2, 1996, PITTS paged the "SVRR [FBI]" and, during the telephone conversation that followed, the UCA and PITTS spoke substantially as follows:

PITTS: I was wondering if it would be able ah, if it would be possible for me to pick up a payment, ah, sometime in the near future?

UCA: Ok, ah, what are your needs, Edwin?

PITTS: Ah just for the material that I've ah, delivered.

UCA: Right. Did you have a certain amount in mind?

PITTS: Ah, well, ah, I believe uh, I have the list you gave me ah, whatever you feel is equitable.

Later in the conversation they continue substantially as follows:

UCA: Is, is eh, equitable. Ok, ok, I will tell this to my superiors. And, ah, is everything ok with you?

PITTS: Ah, yes. Everything is going well. I'm continuing on our project. There's some an… unanticipated uh, difficulty in just locating uh, the information but uh, I'll continue. I…I'll send a progress report with my next uh… report on…on what I found or haven't been able to find.

Later in the conversation they continue substantially as follows:

UCA: Ok. By the by, we received your recent shipment and I understand it was very interesting information.

PITTS: I hope it's ah, good.

93. On or about May 6, 1996, the "SVRR [FBI]" paid PITTS $5,000.00 via Box 318.

May 16, 1996 Drop

94. On or about May 15, 1996, PITTS paged the "SVRR[FBI]," indicating that he would make a drop the next day on or about May 16, 1906. PITTS placed an envelope in Box 318. This envelope contained a videotape classified "Secret." The videotape was of a presentation by an FBI Special Agent to a counterintelligence training class at the FBI Academy in Quantico, Virginia.

June 28, 1996 Drop

95. On or about June 27, 1996, PITTS paged the "SVRR [FBI]" to let them know that he would make a drop the next day. On or about June 28, 1996, he placed an envelope in Box 318. This envelope contained a personnel list for certain FBI employees in the Washington, D.C. area and a computer disk. This disk contained a letter to the person PITTS believed to be his SVRR handler. The letter contained information about three FBI Special Agents who had participated in a particular counterintelligence operation while PITTS was in New York. The letter included the FBI Special Agents home addresses, current office assignments and PITTS' assessment of their personalities. The latter included information such as job satisfaction and, as to one agent, her medical condition. I am aware that the SVRR targets persons with vulnerabilities, such as job dissatisfaction, and that these vulnerabilities can be exploited for recruitment purposes.

The disk also contained lists of FBI personnel being trained at the FBI Academy and the training received; and transfers within the Intelligence Division of the FBI. Finally, PITTS' letter to his "SVRR [FBI]" handler contains the following statements concerning two telecommunications devices:

The secure telephone model III (STU III) is capable of encrypting telephone conversations and facsimile transmissions up to Top Secret level.

I need to know how long you need access to the telephone. I also need to know if you will need access to the key. Finally, I need to know if it will be necessary for me to deliver the telephone to you, or if it can be examined on site.

I can get into a protected area that houses a telephone, but I don't know if I'll be able to disconnect it once inside. I know the location of the key for the unit, but do not have access to where it is located. Access can be gained by manipulating a common tumbler lock, but I do not have those skills. If you have someone who is skilled in entry, I have several preliminary plans for getting them to the location undected [sic]. The key planning factor is how long the examination will take, as it will only be a matter of hours before the unit is missed. Please advise.

I have located several ciphered radios, but they are closely accounted for. Access to the area is closely controlled, so a direct theft of one of the radios would be a very high-risk manuver [sic]. If it is possible to make a facsimile of a radio, it is possible that the facsimile could be substituted for the actual radio, delaying discovery that it is missing. Once the discovery is noticed, security measures will increase dramatically, making future operations much more difficult or impossible. My own assessment is that a direct theft poses greater risks than the potential rewards, but it is a possibility.

I will continue to look for an alternative means of securing a radio that poses fewer operational risks.

July 9, 1996 Drop

96. On or about July 8, 1996, PITTS paged the "SVRR [FBI]" indicating that he would make a drop the next day. As indicated on July 9, 1996, he placed an envelope in Box 318 which contained a computer disk and 112 pages of an FBI Headquarters manual titled "Informal FBI Headquarters Supervisors Manual - Intelligence Division (INTD)." The document was clearly classified "Secret" on the cover, and on numerous internal pages.

The letter on the disk explained that this was only a portion of the manual and the rest would be delivered later (due to the size of the manual). He also requested payment during the week of July 15, 1996.

97. On or about July 22, 1996, the "SVRR [FBI]" paged PITTS, indicating that they would make a drop the following day. This drop included a payment of $5,000.00.

July 25, 1996 Drop

98. On or about July 24, 1996, PITTS paged the "SVRR" indicating that he would make a drop on the following day. As indicated on July 25, 1996 he placed an envelope in Box 318. This envelope contained 110 pages of the Secret FBI manual described above. The drop also contained a computer disk, containing a letter to PITTS' "SVRR [FBI]" handlers. In the letter, PITTS apologized for missing "my appointment last week"; noted that his schedule was unpredictable but believed it could be "managed to avoid unreasonable disruption to our mutual interests"; promised to provide the SVRR "details concerning the [STU-III] telephone you have requested as soon as possible"; and suggested that the Thanksgiving holiday would offer an "excellent window of opportunity" [to smuggle into the FBI Academy an SVRR technical expert].

July 31, 1996 Drop

99. On or about July 30, 1996, PITTS paged the "SVRR [FBI]" indicating that he would make a drop the following day. As indicated, on July 31, 1996, he placed an envelope in Box 318 which contained 192 pages of the Secret FBI manual described above.

August 14, 1996 Drop

100. On or about August 13, 1996, PITTS paged the "SVRR [FBI]" to indicate that he would make a drop the next day. As indicated, on August 14, 1996, he placed an envelope in Box 318. This drop included a computer disk which contained a six page letter. Among "Personnel Actions of Interests," PITTS described a recently retired FBI Special Agent as one whose "knowledge of operations and sources of information over a number of years would be valuable in assessing any past or present security breaches. If the opportunity arises to make an indirect approach, it should be worth the effort." As stated above, vulnerabilities are a key to assessing potential recruitment targets. PITTS also wrote that this agent "tends to be talkative, and appears to be somewhat lonely and isolated. At the time I knew him, most of his social activities revolved around work relationships. Now that he is retired, he will probably feel cut off socially and may be approachable as an indirect source of information."

101. Other information contained on the disk dealt primarily with PITTS' continued efforts toward assisting the "SVRR [FBI]" in gaining access to a STU-III telephone. He told of the location of the STU-III he considered most appropriate, and gave the "SVRR [FBI]" the cypher lock combination to the door of the room housing the telephone. Vehicle and foot access into the Academy were detailed, as well as the possibility of "covert placement (by SVRR personnel] in a class" at the Academy.

102. In this communication, PITTS also noted his desire for a "steady stream of payments," and his concern about being able to "mask" his payments received from the SVRR:

Regarding my reserve, I do not know the amount and it is my understanding that you do not. When I last met with Alex, it was over $100,000. I do not recall discussing the matter with Alex's friends who I met later. The amount of the reserve is not the key point I was trying to raise in my recent communication. I believe I am being treated fairly even though circumstances have made our working relationship more difficult.

My purpose in requesting the recent payments, even if they came from reserve, was to keep a steady stream of payments in place. Given the difficulties we have had maintaining contact in the past, changes in your organizational structure and current conditions, large reserves are of very little current use to me. There are also practical problems that I must deal with if your payments are made in only a few lump sums. It is very difficult to make use of large sums, (over $10,000) without leaving traces of its source. It also is not wise to leave large sums of cash unused, as holding large amounts of cash raises immediate suspicions. The safest way to deal with this is to create a situation where smaller amounts of money can be hidden in assets that are not easily observable but, that can accumulate over a longer period of time. To do this, it is better to deal in smaller amounts but to do so regularly. Regular patterns of spending are difficult to detect, but erratic patterns stand out regardless of the amounts involved. Transactions involving large amounts of money are difficult to hide, even if they are done in cash. Therefore, it is important to my purposes that smaller amounts of cash can regularly be infused into the structures I am using to mask your payments. I suggested use of the reserves because much of the information I have recently provided is not of the quality I have provided in the past and did not wish to imply I expected the same level of payment. However, it is also important that I create and maintain a structure that can accomodate [sic] and mask payments for higher quality material, such as the project we are working on now.

With both my needs and your needs (both monetary and security) in mind, I would ask you to make payments on the material I have provided on either the 10th or 11th of next month. I anticipate I will need one more payment before the end of this year (probablly [sic] November) after additional material is delivered to you.

103. The envelope provided to the "SVRR [FBI]" on August 14, 1996, also contained a color slide of an aerial view of the FBI Training Academy at Quantico, Virginia; eighty seven (87) pages of a Federal Bureau of Investigation manual titled "The Federal Bureau of Investigation Emergency Response Plans, FBI Academy, Quantico, Virginia, Training Division, April, 1996"; and ten (10) FBI Directories.

August 29, 1996 Drop

104. On or about August 29, 1996, PITTS placed an envelope in Box 318. This envelope contained a computer disk and four maps which correlated with information on the disk. On the disk, PITTS gave the exact location of "the device you are interested in" [the STU-III telephone detailed above], information concerning security devices near and on the way to the telephone, and various routes to the phone from the outside of the Academy. He gave the pros and cons for each route, stated which he recommended, and marked the routes on the accompanying maps.

105. On or about September 9, 1996, the "SVRR [FBI]" paged PITTS, indicating there would be a drop made on the following day. On or about September 10, 1996, PITTS was paid $5,000.00 by the "SVRR [FBI]."

September 18, 1996 Drop

106. On or about September 17, 1996, PITTS paged the "SVRR [FBI]" to indicate that he would make a drop the following day. On September 18, 1996, as indicated, PITTS placed an envelope in Box 318. This envelope contained a computer disk and five pages of technical information relating to FBI radios and telephones, including radio frequencies and channels used at the FBI Academy, FBI Headquarters, Washington Field Office, Philadelphia, Pittsburgh, Richmond and New York Divisions.

107. The disk contained information regarding transfers within the FBI Intelligence Division and National Security Division training instructors and attendees at the FBI Academy, including some home addresses and telephone numbers. PITTS highlighted

one individual as someone who "may be of significant interest to you." PITTS also gave extensive information on an FBI espionage investigation of an individual who passed "Top Secret" military information to the Soviets. PITTS continued in his efforts to plan the compromise of a STU-III telephone by recommending a date and method of entry for the SVRR technician, including a particular method to smuggle in the SVRR technician.

September 25, 1996 Drop

108. On or about September 24, 1996, PITTS paged the "SVRR [FBI]" indicating that he would be making a drop the following day. As indicated on or about September 25, 1996, PITTS placed an envelope in Box 318. This envelope contained a computer disk and several telephone directories for the FBI and it's field divisions.

The disk contained detailed information about the STU-III telephone and the best dates for the SVRR technician to enter the FBI Academy. PITTS offered a key to the Academy and a coded card which would allow unaccompanied access to the Academy.

October 6, 1996 Drop

109. On or about October 5, 1996 PITTS paged the "SVRR [FBI]" to indicate that he would make a drop the following day. On or about October 6, 1996, PITTS placed an envelope in Box 318. This envelope contained a computer disk containing a letter which detailed PITTS' continued planning for the entry of the SVRR technician. PITTS stated that "he was in the process of assessing security measures" for the building containing the STU-III. Also enclosed in the envelope were telephone directories and assignment charts for various divisions within the FBI.

110. In this same drop, PITTS enclosed a nineteen page FBI Intelligence Division report titled "Counterintelligence Techniques: Identifying an Intelligence Officer." This document is classified "Secret" in its entirety and, in my opinion, is related to the national defense, as that term is used in Title 18, United States Code, Section 794.

October 16, 1996 Drop

111. On or about October 15, 1996, PITTS paged the "SVRR [FBI]," indicating that he would be making a drop the next day. On or about October 16, 1996, PITTS placed an envelope in Box 318. The envelope contained a computer disk, a key, a hand drawn map with "target" written on it, and a printed FBI Academy map with handwritten notes. An FBI Special Agent verified that the key unlocked an outside door to the FBI Academy.

112. The disk contained information on the best date and time for the SVRR technician to enter the academy, according to staffing and security procedures around the "target area," and suggested a pick up point for the SVRR technician. PITTS offered to obtain an identification card and uniform for the technician to ensure the success of the operation.

113. On or about November 4, 1996, the "SVRR [FBI]" paged PITTS to indicate that there would be a drop for him the next day. On or about November 5, 1996, the "SVRR [FBI]" paid PITTS $5,000.00 via Box 318.

114. Along with the November 5, 1995, payment was a computer disk containing a letter from PITTS' "SVRR [FBI]" handlers. In the letter, the "SVRR [FBI]" told PITTS that it wished to have PITTS' assistance in a "related effort to defeat secure telephones" and that PITTS would be provided a device for this purpose.

115. On November 10, 1996, PITTS was provided by his "SVRR [FBI]" handlers a STU-III handset which PITTS was told had been "modified." PITTS was requested to exchange it with the STU-III handset at the FBI Academy and to deliver the handset "through normal method" for "modifications."

November 12, 1996 Drop

116. On or about November 12, 1996, PITTS placed an envelope in Box 318. This envelope contained an FBI Intelligence Division identification badge, number 784046. The badge is identifiable as PITTS' by his name and photo on the front. This type of badge is used by FBI employees and is considered to be Bureau property. This badge allows entry onto the FBI Academy grounds, as well as unaccompanied entry into the Academy buildings. It also provides bonafides for a person while walking through the Academy as all students, instructors, and visitors are required to wear a badge of some type while inside the Academy.

November 26, 1996 Drop

117. On or about November 26, 1996, PITTS placed an envelope in Box 318. It contained a computer disk

containing a letter to the person PITTS believed to be his SVRR handler. In the letter, PITTS referred to the STU-III handset and said:

> The device has been recieved [sic] and is ready for installation. A window of opportunity exists to install the device, and expect installation by December 2 or 3.

Stealing the STU-III Handset

118. On or about November 29, 1996, PITTS stole a handset from a STU-III telecommunications device from the FBI Academy and replaced it with the supposedly "modified" handset provided to him by his "SVRR [FBI]" handlers.

December 4, 1996 Drop

119. On or about December 3, 1996, PITTS paged the "SVRR [FBI]" to indicate that he would make a drop the next day. On or about December 4, 1996, PITTS made a drop via Box 318. The box he dropped included the handset which he had stolen from the FBI Academy.

The Final Drop

120. On December 12, 1996, PITTS paged the "SVRR [FBI]" indicating that he would make a drop the next day. On December 13, 1996, PITTS placed an envelope in Box 318. In the envelope was a computer disk containing a letter to PITTS' "SVRR [FBI]" handler. Among other things, the letter said:

> *Please understand I no longer have direct access to the files concerning the events that took place during that period [of his New York assignment] and I believe I have provided you with everything that I was aware of.*

121. The "false flag" operation described above began on or about August 12, 1995, and continued to on or about December 13, 1996. During this 16 month time period, PITTS made 22 drops of FBI internal information and documents, of both a classified and unclassified nature, held nine telephone conversations and two face-to-face meetings with his "SVRR [FBI]" handlers, and accepted payment of $65,000 for these services. At no time was PITTS authorized to divulge or convey such documents and information to unauthorized persons or to persons he believed to be unauthorized persons, or to attempt to compromise the security of this information.

Intent to Escape

122. On or about November 2, 1995, during a physical search of Room B-103, FBI Academy, Quantico Marine Base, Quantico, Virginia, the following information relating to an escape plan was found in the hard drive of PITTS' personally owned computer [typed, as in the original]:

Personal security is a greater concern now due to suspicions that may have been raised by our direct communication and the greater possibility of security breakdowns since our previous exchanges. I am developing an emergency escape plan, in the event it needs to be used on short notice. If you wish me to contact you in such an event, please advise me of a point of contact, preferably outside this country, where I should make the contact. Under my working plan, it will take five to six weeks between instituting the plan and being in a position to make contact. To avoid possible security breaches, I will take total responsibility for extracting myself, and only need to know any final point at which you want me to arrive. If it can be passed, I need 35 to 40K from my account to fund the plan and use as a reserve to be used if the plan must be put into effect. Let me emphasize that my plan will only be put into effect as a final extreme measure when all other safeguards

123. In a December 6, 1996, telephone conversation between PITTS and his "SVRR [FBI]" handler, PITTS indicated that it was getting "close to that time" when he would need a passport prepared by the SVRR, and that he would provide the SVRR with a photograph.

124. Based on the above facts and circumstances I believe there is probable cause that EARL EDWIN PITTS committed the following violations of federal criminal law:

A. Conspiracy to Commit Espionage, in violation of Title 18 United States Code Section 794(c);

B. Attempted Espionage in violation of Title 18 United States Code Section 794(a);

C. Communication of Classified Information by Government Officer of Employee, in violation of Title 50 United States Code Section 783(a); and

D. Conveyance Without Authority of Government Property, in violation of Title 18 United States Code Section 641.

Items to be Searched and Seized

125. Based on my training and experience, I know that:

a. Agents of foreign intelligence services maintain records, notes, bank records, financial statements, calendars, journals, maps, instructions, classified documents, and other papers or documents relating to the transmittal of national defense and classified intelligence information to foreign governments and intelligence services. The aforementioned records, notes, bank records, financial statements, calendars, journals, maps, instructions, classified documents, and other papers or documents are maintained, albeit often secreted, on their persons, in and around their residences, places of employment, in home and office computers, automobiles, and in other remote locations, such as safe deposit boxes and storage facilities.

b. Agents of foreign intelligence services often utilize espionage paraphernalia, including devices designed to conceal and transmit national defense and classified intelligence information. These paraphernalia and devices include materials used by espionage agents to communicate between each other and with a foreign government, to wit: coded pads, secret writing paper, microdots, microfiche together with instructions in the use of these materials, recording and electronic transmittal equipment, chemicals used to develop coded and secret messages, computers, computer disks, cameras, film, books, records, documents, and papers. The information which is frequently passed or recorded through such methods often includes:

1) national defense and classified intelligence information;

2) the identities of other foreign espionage agents and intelligence officers;.

3) financial transactions including payments to foreign espionage agents and hidden financial accounts;

4) Records of previous illicit espionage transactions; and

5) the source and disposition of national defense and classified intelligence information.

c. Agents of foreign intelligence services routinely conceal in their residences large amounts of U.S. and foreign currency, financial instruments, precious metals, jewelry, and other items of value and/or proceeds of illegal espionage transactions. They also conceal records relating to hidden foreign and domestic bank and financial accounts, including accounts in fictitious names.

d. It is common for agents of foreign intelligence services to secrete national defense and classified documents and materials, clandestine communications devices and instructions, contact instructions, codes, telephone numbers, maps, photographs, other papers and materials relating to communications procedures, and proceeds and records of illegal espionage transactions in secure, hidden locations and compartments within their residences, places of employment, safe deposit boxes, and/or motor vehicles, including hidden compartments within motor vehicles, for ready access and to conceal such items from law enforcement authorities.

e. Agents of foreign intelligence services are not unlike any other individual in our society in that they maintain documents and records. These documents and records will normally be maintained for long periods of time regardless of whether their value to the agent has diminished. These persons maintain documents and records which will identify and corroborate travel both in the United states and abroad made in connection with foreign intelligence activity, including personal meets with foreign intelligence officers. These documents and records include passports,

visas, calendars, journals, date books, telephone numbers, credit cards, hotel receipts, airline records, correspondence, carbon copies of money orders and cashier's checks evidencing large cash expenditures, and accounts and records in fictitious names.

f. Agents of foreign intelligence services often maintain identity documents, including those utilizing fictitious identities, U.S. and foreign currency, instructions, maps, photographs, U.S. and foreign bank accounts access numbers and instructions, and other papers and materials relating emergency contact procedures and escape plans.

126. Based on the foregoing, I believe there is probable cause that evidence, fruits, instrumentality's, and proceeds of this offense/these offenses are located in:

a. Premises known and described as a single family residence located at 13415 Fox Chase Lane, Spotsylvania, Virginia, 22553 (as more fully described in Attachment A), which is within the Eastern District of Virginia;

b. Premises known and described as Room B-103, Building 19, Behavioral Science Unit, FBI Academy, Quantico Marine Base, Quantico, Virginia (as more fully described in Attachment B) which is within the Eastern District of Virginia;

c. One 1992 Chevrolet S-10 Pick-up Truck, bearing Virginia registration KVI-582, VIN:lGCCS19R7N2l48561, which based on recent observation by FBI Special Agents and surveillance personnel presently is located at 13415 Fox Chase Lane, Spotsylvania, Virginia, 22553;

d. One 1996 Honda Accord, bearing Virginia reg. OXK-347, VIN:lHGCD5636TA1.12429, which based on recent observation by FBI Special Agents and surveillance personnel presently is located at 13415 Fox Chase Lane, Spotsylvania, Virginia, 22553;

e. One storage unit, numbered A425, located at 7400 Alban Station Boulevard, Springfield, Virginia, 22150 (as more fully described in Attachment C);

f. One storage unit,, numbered D13, located at U-Stor-It Mini Storage, 3662 1/2 Jefferson Davis Highway, Fredericksburg, Virginia, 22408 (as more fully described in Attachment D); and

g. One safety deposit box, numbered 114, located at the Central Fidelity Bank, 4230 Plank Road, Fredericksburg, Virginia, 22407.

Warrants Requested

127. Based on the foregoing, I respectfully request the following:

a. Warrant for the Arrest of:
EARL EDWIN PITTS
DOB: September 23, 1953,
SSAN: 486-62-7841;

for violations of Title 18, United States Code (USC), Sections 794(a), 794(c) and 641, and Title 50, United States Code, Section 783(a).

b. Search Warrants for:

1) Premises known and described as a single family residence located at 13415 Fox Chase Laner Spotslvania, Virginia, 22553 (as more fully described in Attachment A), which is within the Eastern District of Virginia;

2) Premises known and described as Room B-103, Building 19, Behavioral Science Unit FBI Academy, Quantico Marine Base, Quantico, Virginia (as more fully described in Attachment B), which is within the Eastern District of Virginia;

3) One 1992 Chevrolet S-10 Pick-up truck, bearing Virginia registration NVI-582, VIN:lGCCS19R7N2148561 which based on recent observation by FBI Special Agents and surveillance personnel is presently located at 13415 Fox Chase Lane, Spotsylvania, Virginia 22553;

4) One 1996 Honda Accord sedan, bearing Virginia registration OXK-347,

VIN:lHGCD5636TA112429, which based on recent observation by FBI Special Agents and surveillance personnel is presently located at 13415 Fox Chase Lane, Spotsylvania, Virginia, 22553;

5) One storage unit, numbered A425, located at Public Storage, 7400 Alban Station Boulevard, Springfleld, Virginia, 22150 (as more fully described in Attachment C);

6) One storage unit, numbered D13, located at U-Stor-It Mini Storage, 3662 1/2 Jefferson Davis Highway, Fredericksburg, Virginia, 22408 (as more fully described in Attachment D); and

7) One safety deposit box, numbered 114, located at the Central Fidelity Bank, 4230 Plank Road, Fredericksburg, Virginia 22407.

Items to be searched for are more fully described in Attachment E.

128. The above facts are true and correct to the best of my knowledge and belief.

David G. Lambert, Special Agent
Federal Bureau of Investigation
Subscribed to and
Sworn before me this
17th day of December, 1996

Hon. Thomas Rawles Jones, Jr.
UNITED STATES MAGISTRATE JUDGE

Alexandria, Virginia

ATTACHMENT A
(Residence of EARL EDWIN PITTS)

The residence located on two and one half acres of land with the address 13415 Fox Chase Lane, Spotsylvania, Virginia. It is a single family dwelling facing Fox Chase Lane. The home has two levels above ground and an unfinished basement. The outside of the residence is finished with tan siding and brick and has a two-car garage attached.

The residence is accessed via a paved driveway that extends 215 feet from Fox Chase Lane. The house number "13415" is located on a mailbox at the street.

ATTACHMENT B
(Office space of EARL EDWIN PITTS)

Room B-103, Building 19, Behavioral Science Unit, is located on the 3rd level beneath the gun vault at the FBI Academy, Quantico Marine Base, Quantico, Virginia. The room is accessed by descending in the elevator located in the firearms cleaning area to "3B." On the wall beside B-103 is a sign, "Earl E. Pitts." The office has a single, wooden door and is approximately 15 feet long and 10 feet wide. The office walls are blue; the ceiling is white.

ATTACHMENT C
(Storage space of EARL EDWIN PITTS)

One storage unit, numbered A425, located at Public Storage, 7400 Alban Station Boulevard, Springfield, Virginia, 22150.

Directions to this unit are as follows: go through a locked gate that requires a keypad code. Facing the storage building, turn left and approximately 35-50 yards on the right is a door to enter the building. Take the elevator to the third floor, exit and take two lefts. Unit A425 is on the right.

ATTACHMENT D
(Storage Space of EARL EDWIN PITTS)

One storage unit, numbered D13, located at U-Stor-It Mini Storage, 3662 1/2 Jefferson Davis Highway, Fredericksburg, Virginia, 22408.

The storage facility is located on the Route 1 Bypass, behind Purvis Ford. The facility is surrounded by a 7'-8' fence. Turn left after entering the facility and go to the end of the two buildings.

Unit D13 is in the western-most building on the north end.

ATTACHMENT E
(Items of EARL EDWIN PITTS to be searched)

1) records, notes, bank records, financial statements, calendars, journals, maps, instructions, classified documents, and other papers or documents relating to the transmittal of national defense and classified intelligence information to foreign governments;

2) espionage paraphernalia, including devices designed to conceal and transmit national defense and

classified intelligence information and materials used by espionage agents to communicate among each other and with a foreign government, to wit: coded pads, secret writing paper, microdots, microfiche together with instructions in the use of these materials, recording and electronic transmittal equipment, chemicals used to develop coded or secret messages, computers, computer disks, cameras, film, books, records, documents, and papers which reflect:

a) national defense and classified intelligence information,

b) the identities of other foreign espionage agents and intelligence officers,

c) financial transactions including payments to foreign espionage agents and hidden financial accounts

d) records of previous illicit espionage transactions, and

e) the source and disposition of national defense and classified intelligence information;

3) large amounts of U.S. and foreign currency financial instruments, precious metals, jewelry, and other items of value and/or proceeds of illegal espionage transactions.

4) national defense and classified documents and materials, clandestine communications devices and instructions, contact instructions, codes, telephone numbers, maps, photographs, other papers and materials relating to communications procedures and proceeds and records of illegal espionage transactions;

5) passports, visas, calendars, journals, date books, telephone numbers, address books, credit cards, hotel receipts, airline records, correspondence, carbon copies of money orders and cashier's checks evidencing large cash expenditures, and accounts and records in fictitious names;

6) identity documents, including those utilizing fictitious identities, U.S. and foreign currency, instructions, maps, photographs, U.S. and foreign bank account access numbers and instructions, and other papers and materials relating emergency contact procedures and escape routes;

7) foreign and domestic bank records, including canceled checks, monthly statements, deposit slips, withdrawal slips, wire transfer requests and confirmations, account numbers, addresses, signature cards, credit cards, and credit card statements, and all other financial statements;

8) safety deposit box records, including signature cards, bills, and payment records;

9) financial and investment account records, including statements, investment confirmations, withdrawal and dividend records, and all other-related account records;

10) federal, state, and local tax returns, work sheets, W-2 forms, W-4 forms, 1099 forms, and all related schedules; and

11) records concerning real property purchases, sales, transfers, in the U.S. and foreign countries, including but not limited to deeds, deeds of trust, land contracts, promissory notes, settlement statements, and mortgage documents.

Russian Commentary on Pitts' Arrest

Analysis by Igor Korotchenko under the general headline: "Yet another agent arrested in the United States….This is the way the FBI 'congratulated' the Russian Chekists on their professional holiday." (FBIS translated text from Moscow Nezavisimaya Gazeta (NG), 20 December 1997.)

In line with existing practice, the official spokesman of Russia's Foreign Intelligence Service (SVR) traditionally declined all comment on the arrest in the United States of FBI employee Earl Edwin Pitts of charges of spying for Moscow. Admittedly, Tatyana Smolis, press secretary of the SVR Director, uttered a very remarkable phrase talking with your NG correspondent: "Irrespective of this case, I can say that even having carried out a considerable reduction of our apparatus abroad, we have not lost the high quality of work inherent in our service. It is sometimes possible

to score a greater effect with a smaller number of people."

It will be recalled that this disgraceful episode happened soon after the case of CIA officer Harold Nicholson accused of cooperation for many years with the KGB's PGU (First Main Department) and the SVR was taken to court.

Although the SVR gave up "globalism" after 1991 and closed more than 30 of its stations in Africa, South East Asia, and Latin America, Russian intelligence doctrine still lists the United States among the objects of prime attention. True, the term "Main Adversary" with regard to Washington is no longer used in the official documents of the intelligence service. At the present time, the man in charge of the American area in the SVR's activities is Lt. Gen. Grigoriy Rapota who has the rank of Deputy Director of this Special Service. He keeps daily tabs on the operational subdivisions abroad subordinated to him. The SVR has three "legal" stations operating in the United States under the cover of official Russian institutions in New York, Washington, and San Francisco. Each of them includes several dozen staff members and has a direct channel of coded communication with the SVR headquarters in Yasenevo. The work of diplomatic stations is organized and carried out in three main area—political, economic, and technical-scientific spying.

Furthermore, according to existing expert assessments, the Foreign Intelligence Service has created anywhere from three to seven major illegal stations in the United States and Canada, each of which is in contact with a corresponding Directorate in Yasenevo. The SVR's Foreign Counterintelligence Directorate also has its own apparatus of agents in the United States who operate independently.

Obviously, in order to localize what is already the second exposure of a valuable Russian spy, Yasenevo will set up a special commission to thoroughly investigate the circumstances of what happened. However, the circumstance that the date of Pitt's arrest was not a random choice is now already conspicuous; it comes shortly before 20 December, the day of the Workers of Russian Federation State Security. American counterintelligence has in this manner "congratulated" Russian Chekists on their professional holiday. FBI Director Louis Freeh must have been strongly impressed by the recent press conference of FSB (Federal Security Service) head Nikolay Kovalev where he announced the catching of 39 agents, Russian citizens recruited by Western special services. This was, perhaps, the other reason why the FBI urgently detained Earl Edwin Pitts, who had been actively watched by American counterintelligence.

Economic Espionage Act of 1996

SECTION 1. SHORT TITLE.

This Act may be cited as the "Economic Espionage Act of 1996."

Sec. 101. PROTECTION OF TRADE SECRETS.

(a) IN GENERAL.–Title l8, United States Code, is amended by inserting after chapter 89 the following:

"CHAPTER 90–PROTECTION OF TRADE SECRETS

Sec.
1831. Economic espionage.
1832. Theft of trade secrets.
1833. Exceptions to prohibitions.
1834. Criminal forfeiture.
1835. Orders to preserve confidentiality.
1836. Civil proceedings to enjoin violations.
1837. Conduct outside the United States.
1838. Construction with other laws.
1839. Definitions.
1831. Economic espionage

(a) IN GENERAL.–Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (4), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) ORGANIZATIONS.—Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

1832. Theft of trade secrets

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate of foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more others persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

1833. Exceptions to prohibitions

"This chapter does not prohibit—

"(1) any otherwise lawful activity conducted by a government entity of the United States, a State, or a political subdivision of a State; or

"(2) the reporting of a suspected violation of law to any government entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

1834. Criminal forfeiture

(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentenced imposed, that the person forfeit to the United States—

(1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceedings in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except for subsections (d) and (j) of such section, which shall not apply to forfeitures under this section.

1835. Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the federal rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

1836. Civil proceedings to enjoin violations

(a) The Attorney general may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

1837. Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if—

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or

(2) an act in furtherance of the offense was committed in the United States.

1838. Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful, disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).

1839. Definitions

As used in this chapter—

(1) the term 'foreign instrumentality' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government;

(2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government;

(3) the term 'trade secret' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public; and

(4) the term 'owner', with respect to a trade secret, means the person or entity in which or in which rightful legal or equitable title to, or license in, the trade secret is reposed."

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning part 1 of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

(c) REPORTS.–Not later than 2 years and 4 years after the date of the enactment of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S.C. 10601).

Cold War Espionage in Germany

(*This report has been lightly edited and all classified data deleted.*)

This assessment was tasked by the Department of Defense Damage Assessment Committee, chaired by Mr. John Grimes DASD (CI&SCM)/C3I. This report describes Soviet and East German intelligence agency Cold War espionage, which targeted German industry and how those activities evolved to serious dimensions for Western security. It examines the ongoing Russian espionage efforts still targeting German industry, which cause the loss of key US defense-related technologies provided in bilateral military exchange programs. Finally, the paper raises concerns over the future implications of this continuing harm to the basic security of the nation, providing policy perspectives for decisionmakers.

There was and continues to be a natural tension between the policies that increase international military sales and commercial trade and the security policies that limit nonproliferation and technology transfer. During the Cold War we accepted risk of compromise with military exchange programs. We still accept a high degree of risk with the same programs, while expecting no immediate change to the threat.

For the future there is every indication that additional espionage and resulting loss of key US defense-related technologies will occur. How severe the risk turns out to be can still be affected by a proactive US Governmentwide response, which must ensure a better balance between risk and potential gain.

Many German defense companies have access to US defense technology information. This information is typically transferred to Germany for weapon system coproduction or for the marketing of US defense goods and services through host-nation companies. Defense technology transfers to Germany represent important material support for its key role in the North Atlantic Treaty Organization. During the Cold War, West Germany's eastern border marked the "front line" of the NATO central region. Germany was, and remains, a principal provider of military forces and weapons to the alliance.

The report makes several judgements and observations:

> The espionage threat posed by the East German intelligence services during the 1980's evolved from a collection effort directed primarily at weapon system "hardware." The focus was expanded to high technology applications as well as to hardware.
>
> The combination of high-tech espionage and US budgetary restraint may narrow the qualitative edge of our future military forces to a surprising and dangerous degree.
>
> Even if the possibility of war with Russia is remote, war between the US and other regional powers is quite plausible. Compromised US technology, marketed to these powers by entrepreneurial Russians, is not unthinkable.
>
> And there are economic consequences. Much of the technology stolen is the valuable proprietary information of US companies. These companies depend upon proprietary information for their competitiveness, profitability, even survival.

DASA's Legacy of Spies

MBB is a major subsidiary of Deutsche Aerospace AG (DASA), the aircraft, defense and satellites division of Daimler Benz. DASA was formed in early 1989 to build a "technology group" on the foundations of the Mercedes Benz automotive business. DASA immediately began a series of corporate acquisitions and new joint ventures. Joint ventures already under way included the "Eurofighter" project with British, Italian, Spanish, and other German companies.

In 1991, DASA's defense sales accounted for 50 percent of the corporation's revenue according to press reporting. By 1993 defense sales generated only about 27 percent of revenue. DASA was sharply and adversely affected by the Cold War's end, by efforts to reduce the German Government budget deficit, and by the long-running global recession. In addition to the Eurofighter, DASA's major remaining military programs include a joint venture guided-missile program with France and close links with Aerospatiale in the European military/civilian helicopter project.

MBB: one Company–Many Spies

Dirk Peter Meyer surrendered to the BfV in 1982 and confessed he had been an agent for the MfS for one year.

Dieter Klimm's espionage career ended with his death in February 1990. He had spied for the MfS since April 1983.

Lothar and Katharina Straube were arrested on 11 December 1990 for spying for the MfS for 19 years (1963 to 1982).

Franz Musalik was arrested in October 1990 on espionage charges.

Peter Kraut and his wife Heindrun were arrested for espionage on 1 January 1992.

Manfred Rotsch was arrested in September 1984 as a KGB spy. Rotsch was probably the most productive known KGB spy at MBB. He had been spying for more than 30 years, the last 15 of them at MBB. Three weeks after Rotsch's September 1984 arrest, FRG authorities arrested a second MBB employee and two workers from other West German defense contracting companies. All three were native East Germans suspected of spying for the KGB. Two of the three, including the MBB employee, were released due to lack of criminal evidence.

Helmut Kolasch's espionage career ended in 1984 with the discovery at MBB, which netted Manfred Rotsch and the others. Kolasch went to work in 1978 on a special project Siemens had contracted with Dornier. Siemens was employed by Dornier to collaborate on a study for a test concept of the tactical fighter jet of the 1990s (TFK-90). The TFK-90 was a forerunner of the European Fighter Aircraft (EFA)—now called the Eurofighter 2000. The project with Dornier was similar to the AFT work with MBB.

Something New for the KGB

The Manfred Rotsch case illustrates the excellent ability of the KGB and MfS to obtain sensitive Western military technology information through human sources actually placed within Western defense industries. The Kolasch case indicates a refinement in the KGB's collection objectives during the early 1980s. The KGB wanted data on high-technology applications, as well as the traditional data on hardware Rotsch and his fellow spies at MBB provided so well for so long.

Espionage for State Profit

Werner Stiller, an East German intelligence officer who defected in 1979, reportedly told Western officials the "game plan." By investing about $2 million in spy operations, East Germany could gain about $130 million worth of technology it would otherwise have to buy. Much of the take was reportedly passed along to the Soviet Union.

An excellent example of such espionage against MTU involved Juergen and Marietta Reichwald from 1973 to 1980. Juergen Reichwald was an MTU engineer. MTU jointly manufactured the engine for the Tornado Multi-role Combat Aircraft, along with Britain's Rolls-Royce and Italy's Fiat. The Tornado was a joint venture of the German, British, and West German aerospace industries. In 1980, the Tornado promised to be Western Europe's most advanced war plane. For delivery in 1988, the FRG had ordered 322 of the aircraft, Britain at least 305, and Italy 100. The Reichwalds were sentenced in 1982 to six and a half years (him) and 15 months (her). At the Reichwald's trial, the presiding judge said the couple had betrayed some of West Germany's most sensitive military secrets "because of their lust for money." The court estimated they received at least $60,000 deutsche marks (about US $470 in monthly payments) from 1973 to 1980.

The KGB Takes Over at MTU

The MfS disintegrated in May 1990. At least one well-placed MfS spy in the MTU company immediately agreed to continue spying directly for the KGB. Karlheinz Steppan, who was arrested October 9,1990 for espionage on behalf of the MFS from 1972 until May 5, 1990, apparently agreed to work for the KGB. He was arrested before beginning to work for his new masters. The Steppan case makes clear that the threat to military-related high technology in German industry did not expire with the demise of the East German espionage apparatus.

Undetected Spies

In an October 1990 magazine interview, Kurt Stavenhagen, the oversight official for all German intelligence agencies reported that a number of former

East German operatives were currently working for the KGB. The KGB had also reportedly taken over entire East German spy nets and operational files.

According to Stavenhagen, the MfS and the KGB had always worked closely. The MfS reportedly had placed about 4,000 active spies in West Germany. Many of the former MfS—now KGB spies—were presently dormant. Others were reportedly active and would remain active. Many had not been detected.

A Spy at DLR

The KGB net extended to another high-technology facility affiliated with Deutsche Aerospace—the German Aviation Research Establishment—better known by the acronym "DLR." On September 4,1992 a 56-year-old unnamed employee of the DLR Aviation and Space Flight Test Center at Goettingen was charged with intelligence activities.

The accused man reportedly confessed to having MfS contacts after his incrimination by a former MfS case officer. The accused was reportedly employed by the Goettingen Test Center for more than 20 years and was recruited by the MfS in the mid–1970s.

Both the Federal German prosecutors' office and a spokesman for the DLR head office stated that the accused was the first MfS spy to be detected within the DLR. The DLR spokesman reported, however, that the accused had not been authorized access to any "classified matters."

The DLR is the largest engineering research and development organization in the FRG. It conducts research at facilities in Oberpfaffenhofen near Munich, Braunschweig, Goettingen, Cologne and Stuttgart. Germany-wide, DLR employs about 4,200, to include more than 1,000 scientists. It has an annual operating budget of approximately $600 million deutsche marks (US $375 million).

The DLR is a hybrid organization, carrying out largely government-funded research and development. It is also obliged to transfer the technology developed to industry for commercial application. A principal industrial beneficiary of the DLR is Deutsche Aerospace AG.

The DLR carries out an impressive array of activities, all involving application of aerospace technology in such areas as flight safety, aerodynamics, and propulsion engineering. The DLR is the focus of the FRG's space programs and contributes to the FRG's participation in the European Space Shuttle Program.

An Underestimated Threat?

The nature of the DLR is such that even a spy with no access to classified material is bound to find unclassified material of interest, especially after working there for 20 years. The accused DLR employee with the MfS contacts showed that agents can be found in "unproductive" areas, and may be far more productive than they seem.

The OLMOS System: A Case Study in Technology Application

The OLMOS Maintenance Support Fatigue Monitoring System permits the German Luftwaffe to monitor the life cycle fatigue values of wear items in the engines and airframe of the Tornado aircraft. It will eventually be expanded to helicopters. The OLMOS system permits "on condition" maintenance—an efficiency- increasing and cost-saving innovation— over the old method of maintenance and repair based upon time-change intervals.

Under the old method, parts that are still fully operational must be exchanged for safety reasons. "On condition" maintenance permits part exchanges only when wear—which is dependent on operation—requires. Knowing the wear lessens the number of unforeseeable part failures and renders unnecessary a preventive parts exchange based upon operating hours.

The Dornier OLMOS Fatigue Monitoring System calculates wear with mathematical algorithms of recorded signals and stores the results as cumulative fatigue values on board the aircraft. Because operating costs are the largest part of the total cost of a complex weapons system, automated "on condition" maintenance permits a considerable reduction in total cost.

New Reasons to Spy

Knowing about OLMOS could not help the Soviets shoot down any Tornados if war broke out. However, theft of Western high-technology applications is motivated by economic as well as military considerations.

Knowledge of OLMOS helped the Soviet Union reduce the desperately high cost of operating its own military aircraft fleet. A Soviet version of OLMOS might have been sold to client militaries around the world bringing in much needed hard currency.

According to press reporting "most present-day (1992) Russian intelligence activity against Germany is concentrated on industrial and economic"— not military—secrets. "A special division of the main Russian service run by Yevgeny Primakov is dedicated exclusively to collecting information on economic conditions and developments in Germany, the US and other leading industrial nations."

A Matter of Competition

The recently issued BfV (German Counter-intelligence) 1992 annual report squarely addresses the issue of Russian spying on the West for economic reasons. "Western companies, banks, think tanks and economic journals (now) enjoy the status of top priority targets," said the report. "The aim is to acquire information to modernize Russian enterprises and improve their ability to compete in world markets."

"Since 1991, numerous Russian intelligence officers assigned to Germany have left the service and tried to establish themselves in private enterprise in Russia or in Germany," the BfV report continued. "Not all of these persons have broken with their former employer." According to German Interior Minister Manfred Kanther, Russian intelligence services reduced their "legal" agents in consulates and the embassy (in Bonn) by about a third in 1992. However, the remaining ones "are still believed to be working hard."

The Story of "John" and "Elizabeth Anne"

Of no less concern are the "illegals"— spies who do not work out of embassies, but run networks of agents under cover or false identities.

On April 23, 1992, a man and a woman claiming to be British disembarked from an Aeroflot plane in Helsinki, Finland. Officials became suspicious when both of the "Brits" (identified as "John David A." and "Elizabeth Anne G.") spoke with heavy Eastern European accents. They were carrying $30,000 in cash, a modified short-range radio receiver, and materials used for writing coded messages. Under questioning, the "Brits" admitted to being Russians and Finnish officials expelled them to Russia.

"The two were either going on an assignment for a foreign intelligence service as 'illegals,' or were on their way back from a consultation in Moscow," the 1992 BfV report concluded. "Articles in their luggage that were made in Germany strongly indicated that this could have been their operational area."

The "Hannover Hackers"

From 1986-88, an eight-member ring of German computer "hackers" created a new form of espionage. The Hannover, Germany-based computer enthusiasts, gained access to passwords and codes at some of the West's most sensitive technical research and military installations. They sold the passwords and codes to the KGB. This was the first international computer espionage case to show how much damage could be done by gathering and selling unclassified data.

The "Hannover Hackers" (collectively known herein as the Hackers) started innocently enough. They soon realized, however, that the information they were collecting might be worth something. They all needed the extra money, some to support drug habits. At first they thought about selling the stolen industrial and research data to competing companies. They focused, however, on a potentially more profitable strategy—obtaining the computer access authorizations with the highest privileges at targeted companies and institutions. They commenced operations, approached the Soviets in East Berlin, and began delivering the data.

The Hackers penetrated Dornier, DLR, MBB, and many other German companies and institutions. The KGB gained full knowledge of the computers at these companies and institutions, and how to break into them. The Hackers showed particular interest in Western research institutions potentially associated with weapons of mass destruction (nuclear, chemical, biological)—and in information about atomic accidents, decontamination zones, toxicological experiments, weapons production, and the contents of weapons depots.

The Hackers' downfall began with an accounting error of 75 cents in a computer billing program at LBL in California. A newly assigned astronomer decided to

investigate the 75-cent problem and discovered that a previous user had added a new account. He then began tracking down the user.

LBL officials established a monitoring system to observe the user, identified as "Sventenk." Over the next year, Sventenk attacked about 450 computer systems around the United States, gaining entry into more than 30. He searched for military and defense-related items, and, when successful, copied data from them.

Sventenk was patient and methodical. He usually followed a pattern: attempting to gain super-user access, then searching for keywords, then for the password file, and finally for other network connections. He would regularly check the system status to see what jobs were running—and who was on line—as if to avoid detection by system administrators.

After tracing was accomplished, several of the Hackers under suspicion were brought in for interrogation by FRG authorities. After the necessary work with other governments, the principal Hackers were formally arrested in March 1989. Two of them cooperated with the authorities to avoid prosecution. (An excellent treatment of the whole story of the Hackers is contained in *The Cuckoo's Egg*, by Cliff Stoll.)

And... Spies at The Ministry of Defense

Wolf-Heinrich Prellwitz and Ulrich Steinmann were longtime KGB and MfS spies in the FRG MOD. Prellwitz served 21 years in the Armaments Division In May 1992, Prellwitz was sentenced to 10 years imprisonment for committing "particularly severe acts of treason" and for "corruption." The 58-year-old "former Federal Defense Ministry Official" had reportedly supplied "particularly sensitive Ministry documents to the former GDR for 21 years."

The Prellwitz and Steinmann cases demonstrate that by the mid-1980s, the GDR intelligence services had penetrated the German MOD as well as the industrial sectors. The GDR services, the KGB, and the Russian Foreign Intelligence Service received considerable amounts of high-quality high-technology information of US origin.

The GDR spent 40 years building the intelligence networks that produced the government spies Prellwitz and Steinmann, and the company spies at MBB, Dornier, MTU, and the DLR. From a GDR point of view, it was a considerable success.

Conclusion: Why This Problem Still Matters to the United States

The July 1992 DoD Key Technologies Plan lists eleven "Technology Areas." These areas are considered vital to achieving success in seven Scientific and Technical (S&T) "thrusts." These thrusts are in turn considered crucial toward making significant improvement in US warfighting capability.

The following lists the eleven technology areas:

1. Computers: High performance computing systems (and their software operating systems) providing orders-of-magnitude communications capabilities as a result of improvements in hardware, architectural designs, networking, and computational methods.

2. Software: The tools and techniques that facilitate the timely generation, maintenance, and enhancement of affordable including sofftware for distributed systems, data base software, artificial intelligence, and neural nets.

3. Sensors: Active sensors (with emitters, such as radar and sonar), passive ("silent') sensors (e.g., thermal imagers, systems), and the associated signal and image processing.

4. Communications Networks: The timely, reliable, and secure production and worldwide dissemination of information, using DoD consumers, in support of joint—Service mission planning, simulation, rehearsal, and execution.

5. Electronic: Ultra-small (nano-scale) electronic and devices optoelectronic devices, combined with electronic packaging and photonics, for high speed computers, data storage modules, communication systems, advanced sensors, signal processing, radar, imaging systems, and automatic control.

6. Environmental Effects: The study, modeling, and simulation of atmospheric, oceanic, terrestrial, and space environmental effects, both natural and man-made, including the interaction of a weapon system with its operating medium and man-produced phenomena such as obscurants found on the battlefield.

7. Materials and Processes: Development of man-made materials (e.g., composites, electronic and photonic materials, smart materials) for improved structures, higher temperature engines, signature reduction, and electronics, and the synthesis and processing required for their application.

8. Energy Storage: The safe, compact storage of electrical or chemical energy, inluding energetic materials for military systems.

9. Propulsion and Energy Conversion: The efficient conversion of stored energy into usable forms, as in fuel efficient aircraft turbine engines and hypersonic systems.

10. Design Automation: Computer-aided design, concurrent engineering, Automation simulation, and modeling; including the computational aspects of fluid dynamics, electromagnetics, advanced structures, structural dynamics, and other automated design processes.

11. Human-System: The machine integration and interpretation of interfaces data and its presentation in a form convenient to the human operator; displays; human intelligence emulated in computational devices; and simulation and synthetic environments.

Exploiting the US Strategy

US Defense S&T Strategy places the highest priority on achieving goals in six technology areas. The six areas (and thrusts) are:

Software (Precision Strike)

Sensors (Air Superiority and Defense/Sea Control and Undersea Superiority)

Communications Networking (Global Surveillance and Communications)

Materials and Processes (Advanced Land Combat)

Design Automation (Technology for Affordability)

Human-System Interface (Synthetic Environments)

Keeping the Game Close

There are at least several possible explanations for the apparent correspondence between our S&T Strategy and their collection objectives. Soviet and GDR leaders apparently intended their espionage to help prevent the West from secretly developing any potentially war-winning military technologies. They also apparently wanted to help prevent or reduce any "technology gaps" between the military forces of the West and East. Such gaps could be used by the West to the political disadvantage of the East.

The evidence indicates the Soviet and GDR leadership wanted to avoid spending the time and money associated with high-technology research and development. They also apparently wanted to apply selected technologies to their own military and commercial products.

Yesterday's Problem?

There is an urge to conclude that the problem of residual KGB and MfS spies in Germany now represents a very manageable risk for US national security. Reasons for such a conclusion may include:

The Warsaw Pact has "gone away." Chances for a major war in Europe presently appear low.

Unification of Germany, and the demise of KGB and MfS, mean that the problem will go away by itself. As the old spies die off, espionage will peter out.

Current political and economic developments in the Russia are not unfavorable. However, if hostile forces emerge to control Russia and if

Russia presents a major new military threat we will know about it well in advance.

If a serious threat develops, any US key technology stolen by spies in earlier years will be more than matched by continuing advances in US defense technology. Our military forces will still possess a significant qualitative edge.

The political, military, and economic future of the former Soviet Union and Warsaw Pact countries is far from certain. Prudence dictates caution about Russia and the East for the next several years. If Russia again presents a serious military threat, the threat may not appear clearly and with sufficient warning. Military threats are often protracted and ambiguous. In the future, serious and continuing losses of US key technologies through espionage and other means could be an important factor undermining international security. This could contribute to military confrontation and increased risk of war.

Even if war with Russia is now remote, war between the US and other regional powers is far more plausible. Stolen United States key technology, marketed to other powers by entrepreneurial Russians, is not unthinkable.

The qualitative edge our military forces have traditionally enjoyed over adversaries is the product of a long-term national commitment to developing key technologies for defense. In today's US budgetary climate, there is no guarantee the nation will be able to sustain the traditional commitment; the future qualitative edge of our military forces is far from assured. The combination of high-tech espionage and budgetary restraint may narrow the qualitative edge of our future forces to a surprising and dangerous degree.

Much of the stolen technology constitutes the valuable proprietary information of US companies. These companies depend upon proprietary information for their competitiveness, profitability, even survival. Much of the capital used by these companies to develop the technologies originated with the US taxpayer.

Department of Defense Directive

May 22, 1997

SUBJECT: DoD Counterintelligence (CI)

References: (a) DoD Directive 5240.2, subject as above, June 6, 1983 (hereby canceled)

(b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981

(c) Presidential Decision Directive/NSC-24, "U.S. Counterintelligence Effectiveness," May 3, 1994

(d) DoD Directive 5137.1, "Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)," February 12, 1992

(e) through (bb), see enclosure 1

A. REISSUANCE AND PURPOSE

1. Reissues reference (a) and implements Section 1.11 of reference (b) as it pertains to the assignment of CI responsibilities to the Defense Intelligence Agency (DIA), National Security Agency (ASA), the Military Departments, and offices referenced in that section.

2. Integrates DoD CI capabilities and coordination procedures into a national CI structure under the direction of the National Security Council (NSC) under reference (c).

3. Establishes and maintains a comprehensive, integrated, and coordinated CI effort within the Department of Defense, pursuant to the responsibilities and authorities assigned to the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD9C3I)) in reference (d).

4. Assigns responsibilities to the DoD Components for the direction, management, coordination, and control of CI activities conducted under the authority of references (b), (d), (e) and this Directive.

5. Establishes the Defense Counterintelligence Board (DCIB).

B. APPLICABILITY

This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

C. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

D. POLICY

It is DoD policy that:

1. CI activities shall be undertaken to detect, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against the Department of Defense, its personnel, information, materiel, facilities and activities.

2. CI activities shall be conducted in accordance with applicable statutes, E.O. 12333 (reference (b)) and DoD issuances that govern and establish guidelines and restrictions for these activities, to include procedures issued under DoD Directive 5240.1 (reference (f)) that govern, among other things, CI activities that affect U.S. persons, as contained in DoD 5240.1-R.

3. CI activities shall be coordinated and conducted within the United States in accordance with the Memorandum of Agreement (MOA) and its supplement between the Attorney General and the Secretary of Defense (references (h) and (i)), and outside the United States between the Secretary of Defense and Director of Central Intelligence in accordance with the Director of Central Intelligence Directive 5/1 and its supplement (references (j) and (k)).

4. Military Department CI elements are under the command and control of their respective Military Department Secretaries, so as to carry out their statutory authorities and responsibilities under 10 U.S.C.162(a)(2) (reference (1)) and 10 U.S.C.3013(c)(7), 5013(c)(7), and 8013(c)(7) (reference (m)).

5. Combatant Commanders may choose to exercise staff coordination authority over Military Department CI elements deployed in an overseas theater. Staff coordination authority is intended to encompass deconfliction of activities and assurance of unity of effort in attaining the Military Department Secretaries and Combatant Commander's objectives relating to CI. This coordination will normally be accompanied through the assigned CI Staff Officer (CISO), as found in DoD Instruction 5240.10 (reference (n)).

6. If a military operation plan or operation order so specifies, a Combatant Commander or the Combatant Commander's designated joint force commander, may, upon National Command Authority-directed execution, assume operational control of Military Department CI elements assigned to support the operation for the duration of the operation, to include pre-deployment, deployment, and redeployment phases. Under this circumstance, these CI elements come under the Combatant Commander's combatant command authority. However, law enforcement and CI investigations and attendant matters carried out by CI elements remain part of the Military Department's administrative responsibilities. Likewise, for joint training exercise purposes, the joint force commander may assume operational control of assigned CI elements for the purpose and duration of the exercise.

7. The Deputy Assistant Secretary of Defense (Intelligence and Security) (DASD(I&S)) will resolve CI issues, where a Military Department CI entity and a Combatant Commander disagree and when one or both appeal the matter through an appropriate channel to the OSD.

8. CI activities shall be inspected in accordance with DoD Directive 5148.11 (reference (o)).

9.There shall be a DCIB, as described in enclosure 3.

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall delegate to the DASD(I&S) the authority to act for the ASD(C3I) in carrying out CI responsibilities assigned by DoD Directive 5137.1 (reference (d)), as follows:

a. The DASD(I&S) shall:

(1) Oversee development and management of the DoD Foreign CI Program.

(2) Establish and monitor management procedures to improve the effectiveness and efficiency of CI and resource management.

(3) Serve as the OSD Tactical Intelligence and Related Activities (TIARA) Functional Manager for CI programs.

(4) Serve as the Functional Manager for information management matters related to designated CI systems.

(5) Represent DoD CI interests on the National CI Policy Board (NACIPB) under PDD/NSC-24 (reference (c)), when necessary.

(6) Delegate to the Director, CI, the following authority and functions:

(a) Develop DoD CI policy and exercise policy supervision and management of DoD CI programs and activities as defined in this Directive.

b) Act as program manager for DoD FCIP resources, which include resources for the Military Departments, On-Site Inspection Agency (OSIA), DIA, and Defense Investigation Service (DIS).

(c) Serve as functional CI manager to include reviewing and monitoring the progress and effectiveness of CI investigations, offensive operations, collection, analysis and production. Conduct or provide for the conduct of inspections of DoD CI Components; staff oversight of DoD CI components and resolve conflicts between those components; and assign special tasks to the DoD Components as may be necessary to accomplish DoD CI objectives.

(d) Chair the DCIB.

(e) Coordinate DoD CI programs and activities with other U.S. Government organizations.

(f) Ensure adequate CI support is provided to the DoD Components, as necessary, to include support to Special Access Programs and support to Human Intelligence (HUMINT).

(g) Support the DASD(I&S) role as the Functional Manager in areas relating to CI.

(h) Support the DASD(I&S) role as the Functional Manager for the Defense CI Information System.

(i) Be the U.S. National CI Advisor to the Allied Command Europe, for the purposes of consultation and coordination of policy matters.

(j) Support or provide DoD representation on the National CI Policy Board, National CI Operations Board, Operations Chiefs Working Group, Investigations Working Group, and representation to the other national-level CI agencies in accordance with PDD/NSC-24 (reference (c)); and represent the ASD(C3I) on the Secretary's Board on Investigations in accordance with DoD Directive 5105.59 (reference (p)).

(k) Approve or refer to the NSC or NACIPB operations or other CI matters that involve significant policy issues.

b. The Director, DIA, shall:

(1) Conduct analysis and production on foreign intelligence and terrorist threats to meet customer needs within Department of Defense, and contribute to national products of these types as appropriate, in accordance with E.O. 12333 (reference (b)), and within the scope of assigned responsibilities and functions of DIA as described in DoD Directive 5105.21 (reference (q)).

(2) Coordinate the CI production of all DoD CI components as requested by the Director of CI.

(3) Provide CI analytic, production, and database support to the Services as requested.

(4) Serve as the DoD CI Collection Requirements Manager as requested by the Director of CI.

(5) Provide CI staff support to the Chairman of the Joint Chiefs of Staff and the Combatant Commanders as requested by the Director of CI and in conformance with DoD Instruction 5240.10 (reference (n)).

(6) Provide CI staff support to the DoD HUMINT Manager as described in DoD Directive 5200.37 (reference (r)) and ensure CI support is provided to the DoD HUMINT collection program.

(7) Develop, implement and maintain intelligence and CI capabilities designed to assist Commanders in the protection of DoD personnel and facilities from terrorism, in accordance with DoD Directive 0-2000.12 (reference (s)).

(8) Conduct threat and vulnerability analysis and support decisions by commanders or program managers in the implementation of appropriate Operations Security (OPSEC) measures in accordance with DoD Directive 5205.2 (t)).

(9) Assess and provide information systems security threat and vulnerability information to support information operations requirements.

(10) Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director of CI.

c. The Director, DIS, shall:

(1) Integrate CI principles and experience into the DIS security countermeasures missions, which consist of conducting personnel security investigations and serving as the cognizant DoD security authority for the National Industrial Security Program, pursuant to E.O. 12829 (reference (u)).

(2) Assist the defense industry in the recognition and reporting of foreign contacts and collection attempts, and the application of threat-appropriate security countermeasures.

(3) Provide pertinent information on the defense industry to support the production of multidisciplinary intelligence threat analyses as required.

(4) Assist the Military Departments' CI organizations in the protection of critical DoD technologies.

(5) Perform those CI-related responsibilities assigned by the OSD, to include the investigative support to the DoD Components (exclusive of Military Departments) relative to unauthorized disclosures of classified information to the public in accordance with DoD Directive 5210.50 (reference (v)).

(6) Participate in national, international, and interdepartmental boards, committees, and other organizations as requested by the Director of CI.

d. The Command, Control, Communications, Computers and Intelligence Integration Support Activity shall:

(1) Provide CI programmatic analyses and expertise to ASD(C3I) and DASD(I&S) in accordance with DoD Directive 5100.81 (reference (w)), to include consolidation of Military Department and Defense Agency Foreign CI Program submissions and participation in Congressional Budget Justification Book production.

(2) Support planning for CI capabilities, communications, and architectures.

2. The Secretaries of the Military Departments shall:

a. Provide for the conduct, direction, management, coordination, and control of CI activities as outlined in paragraphs E.2.b through E.2.j, below; E.O. 12333 (reference (b)); 10 U.S.C.3013, 5013, 8013 (reference (m)); 10 U.S.C. 535 (reference (x)); Pub.L. 99-145(1985), Section 1223.(reference (y)); and DoD Instruction 5505.3 (reference (z)).

b. Conduct CI investigations of Active and Reserve military personnel and, as provided for in agreements with the Attorney General (references (h) and (i)), DoD civilian employees, who may be subject to judicial and/

or administrative action under applicable Federal law and regulations, including the Uniform Code of Military Justice, 10 U.S.C.801-940 (reference (aa)).

c. Conduct CI operations against foreign intelligence services and organizations.

d. Collect, process, exploit and report information of CI significance to satisfy validated national and tactical CI collection requirements.

e. Conduct CI analysis focusing on support to DoD CI operations and investigations, military operations and force protection, security countermeasures, and national policy and programs.

f. Produce CI assessments, studies, estimates, and other finished products, to support U.S. military commanders, the Department of Defense, and the U.S. Intelligence Community.

g. Develop, implement and maintain antiterrorism programs designed to assist Commanders in the protection of DoD personnel and facilities, in accordance with DoD Directive 0-2000.12 (reference (s)).

h. Conduct threat and vulnerability analysis and support decisions by commanders or program managers in the implementation of appropriate OPSEC measures in accordance with DoD Directive 5205.2 (reference (t)).

i. Assess and provide information systems security threat and vulnerability information to support information operations requirements.

j. Prescribe regulations providing to their military investigative organizations the authority to initiate, conduct, delay, suspend or terminate investigations and ensure Commanders outside those specified CI military organizations do not impede the use of military techniques permissible under law or regulation.

k. Maintain, operate, and manage their respective CI components, in accordance with the authorities and responsibilities assigned by this Directive, and provide personnel, equipment, and facilities that CI missions require.

l. Establish Military Department plans, programs, policies, and procedures to accomplish authorized CI functions.

m. Establish and maintain a worldwide CI capability for the purposes outlined in paragraphs E.2.b through E.2.j., above.

n. Develop CI techniques, methods, and equipment required for CI activities and provide basic and specialized training to CI personnel.

o. Provide CI support to the Combatant Commands, other DoD Components, U.S. Government organizations, and foreign CI and security agencies as provided for in this Directive.

p. Inform periodically the Combatant Commanders on CI investigations and operations through the appropriate CI entity and in coordination with the command CISO to fulfill briefing requirements set forth in this Directive and DoD Instruction 5240.10 (reference (n)).

q. Submit CI operational and investigative data and prepare CI analyses as required by the Director for CI.

r. Establish and maintain liaison with U.S. and foreign CI, security, and law enforcement agencies in accordance with policies formulated in E.O. 12333 (reference (b)); the MOA and its supplement between the Attorney General and the Secretary of Defense (references (h) and (i)); DCID5/1 (reference (j) and the CIA/DoD MOA (reference (k)); and coordinate Military Department programs with other U.S. Government organizations.

s. Participate on DoD, national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director for CI.

3. The Chairman of the Joint Chiefs of Staff shall integrate, where appropriate, CI support into all joint planning programs, systems, exercises, doctrine, strategies, policies, and architectures.

4. The Commanders of the Combatant Commands shall integrate, where appropriate, CI support into all

command planning programs, systems, exercises, doctrine, strategies, policies, and architectures.

5. The Under Secretary of Defense for Acquisition and Technology shall ensure that the Director, OSIA, shall:

a. Provide for the internal security of OSIA's inspection, escort and portal monitoring teams.

b. Participate in the production of multidisciplinary intelligence threat analyses as required.

c. Participate on national, international, and interdepartmental boards, committees, and other organizations involving CI as required by the Director for CI.

6. The Director, National Security Agency/Chief, Central Security Service shall:

a. Collect, process, and disseminate signals intelligence information for CI purposes.

b. Participate in the production of multidisciplinary intelligence threat analyses, as required.

c. Participate on national, international, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director for CI.

7. The Director, National Reconnaissance Office, shall:

a. Utilize its systems to support CI activities and requirements.

b. Support the production of multidisciplinary intelligence threat analyses as required.

c. Participate on DoD, national, and interdepartmental boards, committees, and other organizations involving CI as requested by the Director for CI.

8. The Heads of Other DoD Components shall:

a. Refer to the applicable Military Department CI Agency any CI information involving military personnel assigned to their Components for investigation and disposition. Refer reported CI information involving civilian employees by their Components in the United States to their servicing Military Department CI Agency and, when overseas, to the Military Department responsible for providing administrative and logistical support, in accordance with DoD Directive 5240.6 (reference (bb)).

b. Contact the nearest Military Department CI Agency office for guidance should a question arise as where to refer reported CI information.

F. EFFECTIVE DATE

This Directive is effective immediately.

/s/ John P. White
Deputy Secretary of Defense

ENCLOSURE 1

REFERENCES (continued)

(e) Title 10, United States Code, "Armed Forces."

(f) DoD Directive 5240.1, "DoD Intelligence Activities," April 25, 1988.

(g) DoD 5240.1-R, "Activities of DoD Intelligence Components that Affect United States Persons," December 1982, authorized by DoD Directive 5240.1, April 24, 1988.

(h) "Agreement Governing the Conduct of Defense Department Counterintelligence Activities in Conjunction wit the Federal Bureau of Investigation," between the Attorney General and the Secretary of Defense, April 5, 1979.

(i) Supplement to 1979 FBI/DoD Memorandum of Understanding: "Coordination of Counter-intelligence Matters Between FBI and DoD," June 3, and June 20, 1966.

(j) Director of Central Intelligence Directive 5/1, "Espionage and Counterintelligence Activities Abroad," December 19, 1984.

(k) Memorandum of Agreement Between the Central Intelligence Agency and the Department of Defense

regarding counterintelligence activities abroad, February 3, 1995.

(l) Section 162 et seq. of title 10, United States Code.

(m) Sections 3013, 5013, and 8013 of title 10, United States Code.

(n) DoD Instruction 5240.10, "DoD Counterintelligence Support to Unified and Specified Commands, May 18, 1990.

(o) DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight," July 1, 1992.

(p) DoD Directive 5105.59, "The Secretary's Board on Investigations," September 25, 1995.

(q) DoD Directive 5105.21, "Defense Intelligence Agency," May 19, 1977.

(r) DoD Directive 5200.37, "Centralized Management of the Department of Defense Human Intelligence (HUMINT) Operations," December 18, 1992.

(s) DoD Directive 0-2000.12, "DoD Combating Terrorism Program," September 15, 1996.

(t) DoD 5205.2 "DoD Operations Security Program," July 7, 1983

(u) Executive Order 12829, "National Industrial Security Program," January 6, 1993.

(v) DoD Directive 5210.50, "Unauthorized Disclosure of Classified Information to the Public," February 27, 1992.

(w) DoD Directive 5100.81, "Department of Defense Support Activities," December 5, 1991.

(x) Section 535 of title 10, United States Code.

(y) Section 1223 of Public Law 99-145, "Authority for Independent Criminal Investigations by Navy and Air Force Investigative Units," November 8, 1985.

(z) DoD Instruction 5505.3, "Initiation of Investigations by Military Criminal Investigative Organizations," July 11, 1986.

(aa) Sections 801-940 of title 10, United States Code, "Uniform Code of Military Justice."

(bb) DoD Directive 5240.6, "Counterintelligence Awareness and Briefing Program," July 16, 1996.

ENCLOSURE 2

DEFINITIONS

1. Counterintelligence (CI). Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

2. Counterintelligence (CI) Analysis. CI analysis is the function of assimilating, evaluating, and interpreting information about areas of CI proponency and responsibility. Information derived from all available sources is considered and integrated in the analytical process.

3. Counterintelligence (CI) Collection. The systematic acquisition of information concerning espionage, sabotage, terrorism, and related foreign activities conducted for or on behalf of foreign nations, entities, organizations, or persons and that are directed against or threaten DoD interest.

4. Counterintelligence (CI) Investigation. Includes inquiries and other activities undertaken to determine whether a particular person is acting for, or on behalf of, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

5. Counterintelligence (CI) Operation. Actions taken against foreign intelligence services to counter espionage and other clandestine intelligence activities damaging to the national security.

6. Counterintelligence (CI) Production. The process of analyzing all-source information developed into final product and disseminated—irrespective of media—concerning espionage, other foreign intelligence collection threats, sabotage, terrorism, and other related

threats, to U.S. military commanders, the Department of Defense, and the U.S. intelligence community.

7. Counterintelligence (CI) Support to DoD HUMINT. The application of CI information, knowledge, and experience to prevent foreign intelligence or security services from detecting, neutralizing, or controlling DoD HUMINT plans and operations.

8. Military Department Counterintelligence (CI) Agency. The Military Department CI Agencies include Army CI, the Naval Criminal Investigative Service, and the Air Force Office of Special Investigations.

ENCLOSURE 3

DEFENSE COUNTERINTELLIGENCE (CI) BOARD

1. Organization and Management

a. The DCIB shall be convened and chaired by the Director of CI, Office of the Deputy Assistant Secretary of Defense (Intelligence and Security). The DCIB membership shall include representatives from the OSD; Senior Deputy General Counsel (International Affairs and Intelligence); the Assistant to the Secretary of Defense (Intelligence Oversight); one representative from each of the Military Department CI Agencies; the Defense Investigative Service (DS), the On-Site Inspection Agency (OSIA); and the Defense Intelligence Agency (DIA). Associate DCIB members are the National Security Agency/Central Security Service (NSA/CSS); the National Reconnaissance Office (NRO); Marine Corps Counterintelligence/Human Intelligence (HUMINT) Branch; Joint Staff, J-38/IW Special Technical Operations Division/TSB; DIA's Joint CI Support Branch; Counterintelligence Support Officers (CISOs), as described in DoD Instruction 5240.10 (reference (n)); and a representative of the C4I Integration Support Activity (CISA).

b. The DCIB shall be supported by subcommittees or panels, with participation from those organizations represented on the DCIB. The subcommittee and panel chairs shall be appointed by the chair, DCIB.

2. Functions

a. The DCIB shall advise and assist the DASD(I&S) on CI matters within the purview of E.O.12333 (reference (b)), PDD/NSC-24 (reference (c)), and this Directive; e.g. overseeing the implementation of CI policy; advising on the need for and allocation of CI resources; monitoring and evaluating support functions, such as automated data processing; carrying out specific tasks as outlined by the Chair; and reviewing and evaluating reforms of CI entities, to include functional consolidation, integration, and collocation.

b. The DCIB membership will coordinate their respective CI activities, under the guidance of the DCIB chairman.

Charles Lee Francis Anzalone

Spies

Charles Lee Francis Anzalone

Charles Lee Francis Anzalone, a 23-year-old Marine corporal stationed in Yuma, Arizona, was arrested February 13, 1991, after a four-month investigation and charged with suspicion of attempted espionage.

In November 1990, Anzalone, a telephone linemen, called the Soviet Embassy in Washington to offer his services as a spy (under the pretext of asking about a college scholarship). An FBI agent posing as a KGB officer contacted Anzalone who passed him two technical manuals about cryptographic equipment, a security badge, and guard schedules. Anzalone, who is part Mohawk, told the agents that he hated capitalism, the American Government, and held a grudge against the nation's treatment of native Americans. Anzalone testified that his offering to spy was a ruse to get money from the Soviets.

On May 3, 1991, Anzalone was found guilty of attempted espionage. He was also convicted of adultery with the wife of another Marine stationed in the Persian Gulf and of possession and use of marijuana. He was sentenced to 15 years in prison.

Joseph Garfield Brown and Virginia Jean Baynes

On 27 December 1992, FBI agents arrested Joseph Garfield Brown, former US airman and martial arts instructor and charged him with spying for the Philippine Government. Brown allegedly provided an official there with illegally obtained Secret CIA documents on Iraqi terrorist activities during the Persian Gulf War and assassination plans by a Philippine insurgent group.

The former US airman was arrested at Dulles International Airport after being lured to the United States from the Philippines by undercover FBI agents with the promise of a job teaching self-defense tactics to CIA agents. On the following day he was indicted on three counts of espionage in Federal Court, Alexandria, Virginia.

Brown enlisted in the US Air Force in 1966 and served until 1968. He continued to reside in the Philippines, working as a martial arts instructor for the Department of Tourism until the time of his arrest.

He was accused of obtaining classified documents in 1990 and 1991 in Manila from CIA secretary Virginia Jean Baynes and passing them to a Philippine Government official. An FBI spokesman stated that Baynes pleaded guilty to espionage in Federal Court on 22 May 1992 and is serving a 41-month prison term.

The FBI began its investigation in April 1991, after an internal CIA inquiry determined that Baynes, who joined the Agency in 1987 and who was assigned two years later to the American Embassy in Manila, had passed two or three classified documents to Brown. Baynes had met Brown when she enrolled in a karate class which he taught at an embassy annex. According to Baynes, as the friendship between her and Brown grew in the late summer of 1990, he asked her to obtain CIA information on assassinations planned by an insurgent group that were to be carried out in the Philippines. Baynes, who held a Top Secret clearance, complied with his request by removing secret documents from the embassy.

Jeffrey M. Carney

Jeffrey M. Carney, a former intelligence specialist with the Air Force, was sentenced at a General Court Martial December 1991, to 38 years. He pleaded guilty to charges of espionage, conspiracy, and desertion.

Carney entered the Air Force in Berlin where he was a linguist. While at Tempelhof, he began copying classified documents, which he then provided to the East German Ministry for State Security (Stasi). In 1984 he was transferred to Goodfellow AFB in Texas where he worked as an instructor while continuing to spy for East Germany.

After defecting to East Germany in 1985, he continued to aid the Communists by intercepting and translating official telephone communications of US military commanders and embassy officials in Berlin. Carney is a complex personality who became disillusioned with the Air Force. He originally intended to defect to East Germany, but allowed himself to be drawn into espionage by East German agents who expertly manipulated him and claimed his complete loyalty. He was apprehended in Berlin in April 1991 by Air Force Office of Special Investigation agents.

Mark Goldberg

In the late 1980s, a French computer engineer, Mark Goldberg, came to the United States under a program run by the French Ministry of Foreign Affairs that arranged for young Frenchmen to do alternative military service overseas. He was paid a stipend by the French Government, and part of his responsibility under the program was to write reports for the French Government about his work experiences. He worked for a brief period of time for a software company in Connecticut, a wholly owned subsidiary of the French state-owned firm Thompson. Then he joined Renaissance Software, Inc., of Palto Alto, California, a start-up company with fewer than 20 employees specializing in risk management software used by financial traders and banks.

One night, not long before Goldberg was scheduled to return to France on 8 July 1990, he came to the office and copied Renaissance's computer source code. Not long before this, company officials had become suspicious of Goldberg and rigged the computer system and copying machine to detect any theft attempts. The

next day, company officials were able to trace exactly what Goldberg had downloaded.

Goldberg was arrested at the San Francisco airport while waiting for a Paris-bound flight. On 17 July 1990, the Assistant US Attorney Northern District of California, declined to prosecute Goldberg because Goldberg did not place the stolen computer codes into interstate commerce. The US Attorney recommended that the case could be more appropriately prosecuted locally.

On 3 December 1990, Goldberg pleaded guilty in California court to two felony counts of theft and attempted theft of trade secrets. He received a suspended sentence and was allowed to return to France in March 1991 to complete the remaining 400 hours of his 1,000-hour sentence of community service. It never became completely clear whether Goldberg was working for the French Government to steal US technology, but there are many indicators pointing to that possibility.

Douglas Frederick Groat

On 3 April 1998, the FBI arrested Douglas Frederick Groat, a 50-year old former CIA employee, on charges of espionage. Groat is accused of providing information to two foreign governments on how US intelligence successfully cracked their codes.

At a news conference, following Groat's arraignment, US Attorney Wilma A. Lewis said that during his 16-year career with the CIA, Groat "participated in classified covert operations." Other US officials said that Groat worked in units that broke or stole foreign codes.

Groat joined the CIA in 1980. Prior to his CIA employment, he spent five years in the army and held jobs as a police officer, prison guard, process server and deputy US marshal. Groat is the third former or current CIA employee arrested for espionage in the last four years.

Groat was actually indicted on October 31, 1996 in the United States District Court for the District of Columbia. In the indictment, the Grand Jury charged that:

Count One—From on or about March 24, 1997, until in or about April 1997, in the District of Columbia and elsewhere, the defendant, Douglas Fred Groat, did knowingly and willfully communicate, deliver and transmit, and attempt to communicate, deliver, and transmit to "Foreign Government A," and to representatives, officers and agents thereof, a document, writing and information relating to the national defense, that is, information concerning the targeting and compromise of the cryptographic systems of "Foreign Country A" by the United States, with intent and reason to believe that said information was to be used to the injury of the United States and to the advantage of a foreign nation, that is, "Foreign Government A."

Count Two—From on or about March 24, 1997 until in or about April 1997, in the District of Columbia and elsewhere, the defendant, Douglas Fred Groat, did knowingly and willfully communicate, furnish, transmit, and otherwise make available to an unauthorized person, namely representatives, agents and employees of "Foreign Government A," classified information concerning the nature, preparation and use of the cryptographic systems of "Foreign Government A," specifically, the targeting and compromise of the cryptographic systems of "Foreign Government A' by the United States,

(Communications of Cryptographic System Information to a Foreign Government, in violation of Title 18, United States Code, Section 798(a)(1))

Count Three—From on or about March 24, 1997, until in or about April 1997, in the District of Columbia and elsewhere, the defendant, Douglas Fred Groat, did knowingly and willfully communicate, deliver and transmit, and attempt to communicate, deliver, and transmit to "Foreign Government B," and to representatives, officers and agents thereof, a document, writing and information relating to the national defense, that is, information concerning the targeting and compromise of the cryptographic systems of "Foreign Country B" by the United States, with intent and reason to believe that said information was to be used to the injury of the United States and to the advantage of a foreign nation, that is, "Foreign Government B."

Count Four—From on or about March 24, 1997 until in or about April 1997, in the District of Columbia and elsewhere, the defendant, Douglas Fred Groat, did knowingly and willfully communicate, furnish, transmit,

and otherwise make available to an unauthorized person, namely representatives, agents and employees of "Foreign Government B," classified information concerning the nature, preparation and use of the cryptographic systems of "Foreign Government B," specifically, the targeting and compromise of the cryptographic systems of "Foreign Government B" by the United States,

(Communications of Cryptographic System Information to a Foreign Government, in violation of Title 18, United States Code, Section 798(a)(1))

Count Five—From on or about March 24, 1997 until in or about April 1997, in the District of Columbia and elsewhere, the defendant, Douglas Fred Groat, did knowingly and unlawfully attempt to obstruct, delay and affect commerce by extortion, as that term is defined in Title 18, United States Code, Section 1951, in that the defendant, Douglas Fred Groat, did attempt to obtain property of the Central Intelligence Agency, an agency of the United States Government engaged in activities in and affecting foreign commerce by attempting to induce the consent of the Central Intelligence Agency by the wrongful use of actual and threatened fear, including fear of economic and on-economic harm, that is, the defendant did threaten to interfere with Central Intelligence Agency intelligence activities and methods known to him as a result of his employment with the Central Intelligence Agency, by revealing those activities and methods to foreign governments, unless the Central Intelligence (Agency) paid the defendants for his silence in excess of five hundred thousand dollars ($500,000).

(Interference with Commerce by Extortion, in violation of Title 18, United States Code, Section 1951(a))

On 16 April 1998, federal prosecutors said in court that classified documents were found in Groat's recreational vehicle during a FBI search, following his arrest. The prosecutors also said that Groat has "recently considered traveling abroad to seek employment with foreign governments interested in purchasing his classified cryptographic knowledge. The prosecutors' arguments were made in response to Groat's motion to gain release from jail before his trial. The US District Judge, Thomas F. Hogan, rejected the motion and ordered Groat kept in jail.

Groat did not receive any money for his information and did not act out of greed. Rather, this case if one of revenge. The press cites a senior federal official who said that Groat felt slighted and abused by the CIA because he had never been given the assignments he believed he deserved.

A date of 23 September 1998 was set for Groat's trial and arguments concerning legal issues. Groat pleaded not guilty to the five-count indictment, however on 27 July 1998, Grout appeared in the US District Court to plead quilty to one count of attempted extortion. His plea agreement called for a maximum sentence of five years in prison, followed by three years' probation.

Jeff E. Gregory

Jeff E. Gregory, a US Army Staff Sergeant, was arrested on 29 April 1993 at Fort Richardson, Alaska. His arrest resulted from a joint investigation between the FBI and the US Army Intelligence and Security Command. Gregory was the sixth active or former US service member charged with espionage in connection with the Clyde Lee Conrad espionage network that sold US and NATO military secrets to Hungary and Czechoslovakia when those countries were part of the Soviet Bloc.

Gregory is alleged to have been a member of the spy ring which operated out of the 8th Infantry Division, Bad Kreuznach, Germany in the mid-1980s. Gregory was recruited into the spy ring by Roderick James Ramsay, also a former Army sergeant at Bad Kreuznach.

According to the federal complaint against Gregory, while assigned to the 8th Infantry Division in Germany from March 1984 to October 1986, "he helped procure extremely sensitive, classified documents relating to national defense, for transmittal to one or more foreign powers." At the time, Gregory was a staff driver at Bad Kreuznach and helped maintain the commanding general's mobile command center. He was also in charge of updating maps showing military maneuvers and had access to classified messages and correspondence.

According to an FBI official, Gregory once took a military flight bag stuffed with 20 pounds of classified documents. The documents included "war plans" for the United States and NATO. On 28 March 1994, Gregory pleaded guilty to espionage charges.

Frederick Christopher Hamilton

Frederick Christopher Hamilton, a former Defense Intelligence Agency (DIA) analyst, pleaded guilty on 5 February 1993 to the charge of passing to Ecuadorian officials classified US intelligence reports evaluating the military readiness of Peruvian security forces. At the time, Hamilton was a DIA research technician in the defense attache's office in Lima, Peru, a post which he held from 1989 to 1991. He apparently believed that the disclosures could help avert a possible conflict between the two countries. Peru and Ecuador have been disputing territory, sometimes violently, along their mutual border for over 50 years.

Hamilton holds advanced degrees in Spanish and Portuguese. At the time of his arrest, he was employed as a language instructor at a military academy in Virginia. His activities were uncovered by US intelligence agencies after receiving information from a confidential source indicating secrets were being leaked.

Hamilton, who held a Top Secret security clearance while with the DIA, met Ecuadorian representatives in their embassy in Lima on 13 February and 20 May 1991. He passed extremely sensitive information, which disclosed US intelligence operations and the identity of US sources in the region.

"He didn't get any money," said a U.S. official. "He was a very naïve individual who was flattered by the (Ecuadorians)." Hamilton's attorney stated that, "What he thought he was trying to do was prevent a war…. The purpose of disclosing documents that he did was to show the country that was concerned about being attacked that the other country had neither the intent nor the ability to attack."

Hamilton reportedly passed five Secret intelligence reports and orally disclosed the contents of four other classified reports. Under a court agreement, the former DIA employee pleaded guilty to two counts of unlawfully communicating classified information to a foreign country. The agreement specified Hamilton may not appeal the sentence and the Justice Department will not prosecute him for espionage-related crimes.

On 16 April 1993, he was sentenced to 37 months in prison.

Geneva Jones and Dominic Ntube

Geneva Jones, a secretary with a Top Secret clearance in the Department of State's Bureau of Politico-Military Affairs, was arrested on 3 August 1993. On 4 August, the FBI arrested West African journalist Dominic Ntube. On 31 August, she was indicted on 21 counts of theft of government property and one count of transmission of defense information to unauthorized persons. FBI officials said she smuggled classified documents for two years to Ntube, indicted at the same time.

Jones was carrying classified documents with her at the time of arrest. A search of Ntube's apartment by FBI agents discovered thousands of classified cables and 39 CIA documents marked Secret, including documents relating to US military operations in Somalia and Iraq. Some of the material apparently made its way to West African magazines, which had been publishing classified State Department cables for several months.

FBI agents indicated they wiretapped Jones's telephone after several classified US documents were found 10 months earlier in the West African command post of Charles Taylor, leader of a faction seeking to overthrow the Liberian Government. Ntube reportedly faxed 14 documents he received from Jones to the Liberian rebels.

The former State Department employee told the FBI she had been giving Ntube classified cables for about 18 months. In a preliminary hearing, the FBI testified that agents watched her on 16 occasions take documents from the State Department and hide them in newspapers or a grocery bag. During the month she was under surveillance, she allegedly took more than 130 classified documents from her office.

On 31 August,1993, Ntube was indicted with Jones for receiving stolen property and for transmitting national defense information to unauthorized persons. On 3 September, 1993, Jones pleaded not guilty to the charges in Federal District Court.

Peter H. Lee

On 8 December 1997, US Attorney Nora M. Manella announced that a physicist pleaded guilty that day to transmitting classified national defense information to representatives of the People's Republic of China. Dr.

Peter H. Lee, 58, of Manhattan Beach, California, admitted that in 1985, while working as a research physicist at Los Alamos National Laboratory, he traveled to the People's Republic of China. At the time of his trip, Lee, an expert on laser energy, was working on classified projects relating to the simulation of nuclear detonations, which required that he have a security clearance. During meetings with Chinese scientists, Lee provided detailed information about the use of lasers to simulate nuclear detonations, even though Lee knew that this information was classified.

The motive, authorities believe, was not money but national loyalties. Lee "wanted to help the Chinese Government and the Chinese scientists and to do something to advance what he considered to be a poorer, less technologically advanced scientific community," said one law enforcement source. The source further added that "I would characterize (Lee's motives) as an empathy and a sympathy for that country based on his ancestry. He seemed to be eager to help friends back there."

In pleading guilty, Lee admitted that he knew the information was classified, and that by transmitting the information he intended to help the Chinese. "One of the nation's greatest resources is the knowledge possessed by our top scientists," Manella said. "The security of our nation depends on our scientists safeguarding that knowledge. Doctor Lee failed in his duty to protect the information entrusted to him."

In addition to pleading guilty to transmitting national defense information, Lee admitted making a false statement to a government agency. The second charge related to conduct in 1997, when Lee again traveled to the People's Republic of China and lectured on various topics relating to his current employment as a research scientist for TRW, Inc. Following his return to the United States, Lee lied on a security form when he denied that he gave technical talks to the Chinese.

According to Assistant United States Attorney Jonathan S. Shipiro, the information Lee passed in 1985 had important military applications related to nuclear weapons. The information was later declassified.

Lee entered his guilty pleas before US District Judge Terry J. Hatter, who scheduled a sentencing hearing for February 23, 1998. The defendant faces a maximum sentence of 15 years in federal prison and a fine of $250,000. A plea agreement in this case has been filed under seal pursuant to an agreement of the parties.

Kurt G. Lessenthien

After he admitted to trying to sell military secrets to Russia, Petty Officer Kurt G. Lessenthien, a nuclear submarine crewman and instructor at the US Navy's Nuclear Power School in Orlando, Florida, was sentenced to 27 years in prison on 28 October 1996. After Lessenthien made a deal with prosecutors in Norfolk, Virginia, he decided to let a jury determine his sentence hoping it would result in a lighter sentence. Instead, the jury recommended the maximum sentence. He will be eligible for parole after nine years.

Lessenthien had contacted the Russian Embassy in Washington, DC, in March and offered to sell classified nuclear submarine information. Shortly thereafter, an FBI agent posing as a spy contacted Lessenthien and agreed to pay $11,000 for two packages of classified information.

A Navy psychiatrist testified that Lessenthien has a personality disorder making him dependent on women and obsessive about his relationships; however, a Navy prosecutor said Lessenthien spied for money and excitement.

Aluru J. Prasad

An Indian businessman, Aluru J. Prasad, was sentenced on 9 December 1996 to 15 months in prison for spying for the former Soviet Union during the 1980s. The suspected spy pleaded no contest to trying to gather secrets about the US "Star Wars" anti-missile defense system, the stealth bomber, and other classified defense projects.

At the plea hearing, Prasad admitted to working with Subtrahmanyan Kota of Northboro, Massachusetts—an Indian-born software engineer—to steal high-tech information from the Mitre Corporation, including formulas for the paint used to cloak the stealth bomber form radar detection. Earlier in the year, Kota had testified against Prasad and pleaded guilty to wire fraud, three counts of tax evasion, and a charge relating to biotech theft.

Yen Men Kao

On 3 December 1993, the FBI arrested Yen Men Kao, a Chinese national, in Charlotte, North Carolina, as a suspect in a spy ring that unsuccessfully sought secrets on an advanced Navy torpedo and a jet engine. The arrest of Yen by the FBI and Immigration and Naturalization Service agents concluded a six-and-a-half-year investigation that determined that Kao and several other Chinese nationals conspired to steal and export classified and embargoed high-technology items. The attempted espionage targeted the Navy's MK 48 Advanced Capability Torpedo and the F404-400 General Electric jet engine used to power the Navy's Hornet fighter.

According to the FBI, the investigation yielded a significant amount of counterintelligence information, including the identities of numerous suspected intelligence operatives and commercial entities involved in Kao's alleged attempts to illegally acquire US technology. Kao was charged with violating US immigration laws, specifically, a section of the Immigration and Nationality Act that provides for deporting a foreigner involved in any espionage or sabotage activity or seeking to illegally acquire US technology.

Steven J. Lalas

On 3 May 1993, the FBI arrested Steven J. Lalas, a former Department of State communications officer stationed at the US Embassy in Athens, Greece. He was charged with passing sensitive military information to Greek officials. Lalas originally claimed that a Greek military official recruited him in 1991. Lalas said he agreed to cooperate because he feared for the welfare of relatives living in Greece. American authorities later stated that he began spying for the Greek Government in 1977 when he was with the US Army.

Roderick James Ramsay

American authorities estimate that he passed 700 highly classified documents, including papers dealing with plans and readiness for US military strategy in the Balkans and a US assessment of Greece's intentions toward the former Yugoslav. Athens was Lalas' fourth communications posting with the State Department. He had previously served in Belgrade, Istanbul, and in Taiwan.

During his espionage career, he earned a steady income stealing, then selling, Defense Intelligence Agency reports about troop strength, political analyses, and military discussions contained in cables between the US Embassy in Athens and the White House, FBI communications about counterterrorism efforts, and the names and job descriptions of CIA agents stationed overseas. Greek handlers allegedly paid him $20,000 to provide about 240 documents from 1991 to 1993.

The US Government first learned of the espionage activities in February 1993, when an official of the Greek Embassy in the United States made a statement to a State Department officer indicating that he knew the contents of a Secret communication from the US Embassy in Athens to the State Department. Lalas was later identified (through a video monitoring system) stealing documents intended for destruction.

In June 1993, Lalas pleaded guilty to one count of conspiracy to commit espionage and on September 16th was sentenced to 14 years in federal prison without possibility of parole. Prosecutors had recommended the 14-year sentence in return for Lalas' promise to reveal what documents he turned over and to whom. The full extent of his espionage activity was revealed prior to sentencing only after he failed two FBI polygraph examinations.

Roderick James Ramsay

Roderick James Ramsay, a former US Army sergeant, was arrested in Tampa, Florida, on 7 June 1990 and charged with conspiracy to commit espionage.

Ramsay joined the Army in 1981 and was transferred to West Germany in June 1983 where he was recruited by then, Army Sgt. Clyde Lee Conrad. Ramsay received $20,000 for selling military secrets that could have caused the collapse of NATO, Top Secret plans for the defense of Central Europe, the location and use of NATO tactical nuclear weapons, and the ability of NATO's military communications that were passed to Hungary and Czechoslovakia. An FBI official said, "It's one of the most serious breaches ever, it's unprecedented what went over to the other side. The ability to defend ourselves is neutralized because they have all our plans."

Ramsay initially used a 35-mm camera to photograph classified documents, but then switched to more effective videotape. He reportedly recorded a total of about 45 hours of videotape. Ramsay is said to have a high IQ, is multilingual, and has the "ability to recall minute details, facts, and figures from hundreds of volumes of documents." The FBI described him as "brilliant and erratic."

In West Germany he worked as a clerk-typist in the 8th Infantry Division. When arrested he was unemployed, living sometimes at his mother's house and sometimes in his car.

In September 1991 he pleaded guilty and agreed to cooperate with prosecutors. On 28 August 1992 he was sentenced to 36 years in prison. The sentence reflects his cooperation with investigators.

Albert T. Sombolay

Jeffrey Stephen Rondeau

On 22 October 1992, Jeffrey Stephen Rondeau, a US Army sergeant stationed at Bangor, Maine, was arrested in Tampa, Florida. He was charged with espionage for providing US Army and NATO defense secrets, including tactical nuclear weapons' plans, to Hungarian and Czechoslovak intelligence agents from 1985 through 1988. Rondeau was part of the Clyde Lee Conrad spy ring, which operated out the 8th Infantry Division, Bad Kreuznach, Germany, in the mid-1980s.

The inquiry into Rondeau's involvement was aided by the cooperation of Roderick James Ramsay. As a recognition signal, Ramsay reportedly gave Rondeau a torn dollar bill to use when dealing with others in the plot. The US Attorney for the Middle District of Florida said, "The espionage charge in this case is especially serious because it's related to the allied defense of Central Europe, including the use of tactical nuclear weapons and military communications."

The three-count indictment of Rondeau charged that he conspired with Conrad, Ramsay and others to "copy, steal, photopgrah and videotape" documents and sell them to Hungary and Czechoslovakia. The indictment did not specify what amount of money he may have received. On 28 March 1994, Rondeau pleaded guilty to espionage.

Albert T. Sombolay

Albert T. Sombolay, a specialist 4th class with the US Army artillery, pleaded guilty in July 1991 to espionage and aiding the enemy. He was tried by a military judge in Baumholder, Germany, and sentenced to confinement at hard labor for 34 years, reduced to E-1, forfeited all pay and allowances, and received a dishonorable discharge.

Sombolay was born in Zaire, Africa. He became a naturalized US citizen in 1978 and entered the Army in 1985 as a cannon crewman. In December 1990, assigned to the 8th Infantry Division in Baumholder, he contacted the Iraqi and Jordanian Embassies to volunteer his services in support of the "Arab cause." To the Jordanian Embassy in Brussels, he passed information on US troop readiness and promised more information to include videotapes of US equipment and positions in Saudi Arabia. He told the Jordanians that he would be

deployed to Saudi Arabia and could provide them with useful information. To the Iraqi Embassy in Bonn, Germany, he offered the same services, but they did not respond.

On 29 December 1990, Sombolay's unit was deployed to Saudi Arabia, as part of Desert Sheild, without him. Still in Germany, Sombolay continued to contact the Iraqis and provided a Jordanian representative several items of chemical warfare equipment (chemical suit, boots, gloves, and decontamination gear).

His activity was discovered by US Army Military Intelligence. After Sombolay's arrest in March 1991, he admitted to providing Desert Sheild deployment information, military identification cards, and chemical protection equipment to Jordanian officials. He was motivated by money.

Jeffrey Schevitz

In November 1995, a German court in Stuttgart convicted Jeffrey Schevitz, an American systems analyst, of spying for East Germany. At the trial, Schevitz admitted to passing information about West Germany's nuclear policies to the East German intelligence agency between 1977 and 1990. He also claimed that he was working for the Central Intelligence Agency (CIA) as a double agent with the objective of learning Stasi modus operandi. The CIA denied any involvement with Schevitz and a German intelligence officer testified that his service found no connection between CIA and Schevitz.

The prosecutors at the trial revealed that the Stasi gave Schevitz the codename "Robert." During his espionage activities, Schevitz provided information about German nuclear and nonproliferation policies. He obtained his information from contacts with German Government and other officials during his teaching at Berlin's Free University during the 1970s and later when employed as a systems analyst at Germany's Nuclear Research Center in Karlsruhe from 1980 to 1994. Schevitz delivered his information during personal meetings with Stasi officers and by using a dead drop aboard the express train from Basel to Berlin.

The five judge panel announced a suspended sentence of 18 months but did give him three years probation, allowing Schevitz to go free. The court fined him $10,000, which will go to charity, and court costs. Schevitz's plea for leniency influenced the judges. He said that he was attempting to ease the potential conflicts between East and West during the tense 1970s. The prosecutors's statement that the information passed was of little importance also helped.

The German authorities arrested Schevitz's wife, Beatrice Altman, but dropped the charges when she agreed to pay a fine of $7,000.

Three Taiwan Nationals Indicated for Espionage

Kai-Lo Hsu, Technical Director of the Yuen Foong Paper Co. Ltd., in Taipai, and Chester S. Ho, a professor at the National Chiao Tung University, were arrested in Philadelphia on 14 June 1997 on charges relating to an alleged plan to steal trade secrets from the pharmaceutical firm, Bristol-Myers Squibb Company. The two are being held in home detention under a $1 million bond secured by real estate and bank accounts. An arrest warrant was also issued for a third person, Jessica Chou, identified as a manager for business development in Yuen Foong. Her exact location was unknown.

According to the arrest warrant and multiple open sources, Hsu and Ho conspired to illegally acquire, through an FBI undercover agent, plant cell culture technology used to make Taxol, an anticancer drug used to treat ovarian cancer. The 11-count indictment charges that two of the three accused agreed to make a preliminary payment of $400,000 in cash, stock, and royalties to a corrupt Bristol-Myers scientist and a man they thought was a technology-information broker. The broker was an undercover FBI agent and the supposedly corrupt scientist was working with the government.

Hsu was charged with six counts of mail fraud, one count of conspiracy to steal trade secrets, one count of attempted theft of trade secrets, and other violations. Ho was charged with one count of conspiracy to steal trade secrets, one count of attempted theft of trade secrets, and other violations. Chou was charged with mail fraud, conspiracy to steal trade secrets, and other charges. Maximum penalties for the charges range up to 60 years in prison and up to a $2,500,000 fine.

It is uncertain if the attempted deal was sanctioned by high-level executives at Yuen Foong, however, Hsu

allegedly made the comment that his company was diversifying its interests into the area of biotechnology and working on a government project on Taxol technology. A spokesman for Bristol-Myers noted that Taxol is a billion-dollar product around the world and that the cost of losing the technology would have been significant.

A federal judge in October 1997, ordered prosecutors to turn over to the defendants and their lawyers the very documents the defendants are accused of trying to steal. The judge ruled that they needed the information to prepare their defense, and that their right to a fair trial overrides the rights of a company to projtect its trade secrets. Prosecutors are appealing the ruling.

Daniel and Patrick Worthing

On April 18, 1997, Daniel Worthing, of New Kensington, Pennsylvania, became the first person in the United States to be convicted under the Economic Espionage Act. Convicted in February 1997 of conspiracy to possess and deliver trade secrets, Worthing was sentenced to five years' probation, with six months' home confinement. He was also ordered to complete 100 hours of community service and pay a special assessment of $100.

The plot involving the two brothers began unraveling in mid-November 1996 when the chief executive officer of Owens-Corning received a letter from "Dane Davis," offering to sell 19 items of PPG Industries' trade secrets for $1,000. The trade secrets were later identified as customer lists, secret fiberglass formulas, videos of machine operations, blueprints, photographs, and product samples. Unknown to the sender, the Owens-Corning executive forwarded the letter to PPG officials, who contacted the FBI.

On 3 December 1996, the Owens-Corning Company executive received a three-page fax from "Dane Davis," outlining more PPG insider information. A small memo automatically typed on the fax by the sending machine identified it as being sent from PPG's offices. The executive was asked to page the sender if he was interested.

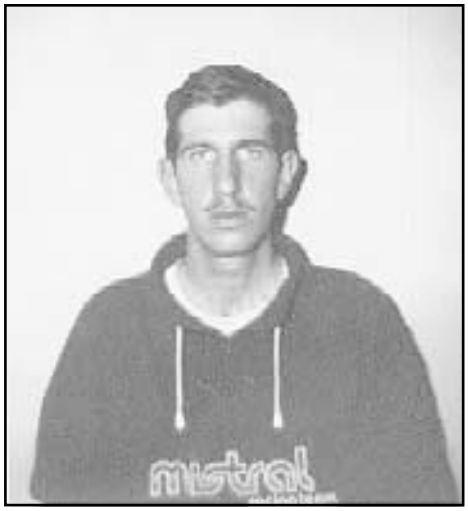
The sender turned out to be Patrick Worthing, who used his own pager number in the fax. Patrick supervised a maintenance crew of about 50 workers who cleaned PPG's fiberglass research center and supplied people to operate prototype machines in suburban Pittsburgh. The crew allegedly had complete access to every office in the facility.

On 7 December 1996, believing they were to meet with a Owens-Corning representative, Patrick and Daniel Worthing were arrested by the FBI. Daniel Worthing, a garbage hauler by trade, said he got involved to protect his brother and to get a percentage of the profits.

Patrick Worthing was sentenced to a 15-month federal prison term in May 1997 for his ill-fated attempt to steal trade secrets from PPG Industries. He was free on bond until he reported to prison.

Charles Schoof and John Haeger

Two US Navy men stationed aboard a ship at the US Naval Amphibious Base at Little Creek, Virginia, received lengthy jail sentences after pleading guilty to conspiring to sell classified information to the Soviets. In proceedings held at the Navy Legal Service Office in Norfolk, Haeger pleaded guilty to conspiracy to commit espionage on 23 April 1990 and on 24 April was sentenced to 19 years in prison, reduction in rate to E-1, forfeiture of all pay and allowances, and a dishonorable discharge. On 24 April, Schoof pleaded guilty to conspiracy to commit espionage and was sentenced to 25 years in prison, reduction in rate to E-1, forfeiture of all pay and allowances, and a dishonorable discharge. Charles Edward Schoof, age

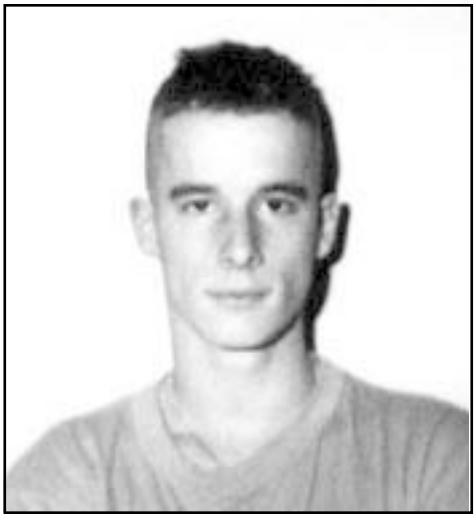


Charles Schoof

21, and John Joseph Haeger, age 20, both Operations Specialists (OS3) were arrested on 1 December 1989 by Naval Criminal Investigative Service (NCIS) special agents.

Both men, assigned to the USS *Fairfax County*, became the focus of an investigation when one of their fellow crewmembers reported what he believed to be suspicious activity by them to the ship's commanding officer. Upon hearing the crewmember's suspicions, the commanding officer immediately initiated an inventory of classified material abroad the vessel. The inventory revealed that classified microfiche containing Secret and NATO Secret material were missing.

After confirming that classified material was missing, the commanding officer notified NCIS. NCIS agents arrested Schoof on board the ship and found him in possession of 12 pieces of microfiche containing six separate publications. An hour later, Haeger was arrested aboard the ship. NCIS later learned that Schoof was planning to either destroy the material or take it to the Soviet Embassy in Washington, DC, that weekend. Schoof was actually preparing to leave the ship when he was arrested.



John Haeger

CI at the End of the 20th Century Bibliography

Andrew, Christopher. *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush*. New York: Harper Collins, 1995.

Bar-Joseph, Uri. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel and Britain*. University Park, PA: The Pennsylvania State University Press, 1995.

Beans, James D. "Marine Corps Counterintelligence: 1990-2000." *American Intelligence Journal* 10:2 (1989): 47-50.

Boren, David L. "Counterintelligence for the 1990's," *American Intelligence Journal* 10:2 (1989): 9-14.

Costello, John and Oleg Tsarev. *Deadly Illusions*. New York: Crown Publishers, 1993.

Deriabin, Peter and T. H. Bagley. *The KGB: Masters of the Soviet Union,* New York: Hippocrene Books, 1990.

Early, Pete. *Confessions of a Spy: The Real Story of Aldrich Ames*. New York: G.P. Putnam's Sons, 1997.

Eftimiades, Nicholas. *Chinese Intelligence Operations*. Annapolis, MD: Naval Institute Press, 1994.

Fialka, John. *War By Other Means: Economic Espionage in America*. New York: W.W. Norton & Company, 1997.

Kalaris, George and Leonard McCoy. "Counter-intelligence for the 1990's," *International Journal of Intelligence and Counterintelligence* 2:2 (1988): 179-187.

Maas, Peter. *Killer Spy: The Inside Story of the FBI's Pursuit and Capture of Aldrich Ames, America's Deadliest Spy*. New York: Warner Books, 1995.

MacKenzie, Angus. *Secrets: The CIA's War at Home*. Berkeley, CA: University of California Press, 1997.

Milano, James V. *Soldiers, Spies and the Rat-Line:America's Undeclared War Against the Soviets*. Washington: Brassey's, 1995.

O'Toole, G.J.A. *Honorable Treachery*. New York: Atlantic Monthly Press, 1991.

Porch, Douglas. *The French Secret Service: A History of French Intelligence From the Dreyfus Affair to the Gulf War*. New York: Farrar, Strauss and Giroux, 1995.

Richelson, Jeffrey T. *A Century of Spies: Intelligence in the Twentieth Century*. New York: Oxford University Press, 1995.

Riebling, Mark. *Wedge, The Secret War Between the FBI and CIA*. New York: Alfred A. Knopf, 1994.

Schachte, W.L., Jr. "NISCOM Counterintelligence Strategy for the 1990's," *American Intelligence Journal* 10:2 (1989) 43-45.

Sessions, William S. "The Evolving Threat. Meeting the Counterintelligence Challenges of the 1990's: A Strategic Issue Facing Our Nation." *American Intelligence Journal* 10:2 (1989): 19-23.

U.S. Congress. Senate. Select Committee on Intelligence. *An Assessment of the Aldrich H. Ames Espionage Case and its Implications for US Intelligence: A Report of the US Senate Select Committee on Intelligence*. Washington, DC: GPO, 1994.

Weiner, Tim, David Johnston and Neil A. Lewis. *Betrayal: The Story of Aldrich Ames, An American Spy*. New York: Random House, 1995.

Weinstein, Sidney T. "The Role of U.S. Counter-intelligence in the Next Decade," *American Intelligence Journal* 10:2 (1989): 33-36.

Westerfield, H. Bradford, ed. *Inside CIA's Private World: Declassified Articles From the Agency's Internal Journal 1955-1992*. New Haven, CT: Yale University Press, 1955.

Wise, David. *Nightmover: How Aldrich Ames Sold the CIA to the KGB for $4.6 Million*. New York: Harper Collins, 1995.

IMPORTANT DATES AND COUNTERINTELLIGENCE EVENTS

CLOSING THE 20TH CENTURY 1990-PRESENT

1990	7 June	Roderick Ramsey, US Army, arrested for spying for Hungary and Czechoslovakia.
	12 June	Clyde Lee Conrad, U.S. Army Sergeant, is convicted of espionage and given life imprisonment.
	16 July	President Bush restructures the President's Foreign Intelligence Advisory Board by shrinking the membership from 15 to six.
	5 October	President George Bush signs off on National Security Directive-47, which tasks CIA, FBI, NSA and the departments of State, Defense and Justice to continue to rebuild US counterintelligence programs.
	5 November	The State department dismisses foreign service officer Felix Bloch who is suspected of spying for the Soviet Union since the early 1970s.
1991	29 March	A major fire damages the US embassy in Moscow.
	22 April	Jeffrey M. Carney, USAF, is arrested for spying for the East German Ministry of State Security.
	30 September	Yevgeniy Primakov named director of the SVRR, the renamed First Chief Directorate, which was the foreign intelligence arm of the old KGB.
	25 December	The Soviet Union dissolves.
1992	21 January	Douglas Tsou, FBI, sentenced to 10 years in prison for spying for Taiwan.
	22 May	Virginia J. Baynes, a CIA employee, pleaded guilty to one count of espionage and was sentenced in October 1992 to 41 months in prison.
	18 September	The existence of the National Reconnaissance Office officially acknowledged.
	22 October	Jeffrey Stephen Rondeau, U.S. Army, arrested and indicted on three counts of espionage. He is believed to be a member of the Clyde Lee Conrad espionage ring.
	27 December	Joseph G. Brown was arrested and charged with passing classified information he received from Virginia J. Baynes to the Philippine Government.

IMPORTANT DATES AND COUNTERINTELLIGENCE EVENTS

CLOSING THE 20TH CENTURY 1990-PRESENT

1993	5 February	Frederick C. Hamilton, DIA official who was arrested for espionage, pled guilty to two counts of espionage and is sentenced to 37 months imprisonment.
	16 April	Frederick Hamilton, Defense Intelligence Agency, sentenced to 37 months in prison for spying for Ecuador.
	29 April	Jeff E. Gregory, Army Staff Sergeant, arrested for espionage. He is believed to be a part of the Clyde Lee Conrad espionage ring.
	30 April	Steven J. Lalas, a Department of State employee, is arrested and charged with passing sensitive military, political, and economic information to Greek officials.
	3 August	Geneva Jones, U.S. Department of State, arrested for Unauthorized Possession of National Defense Information.
1994	21 February	Aldrich "Rick" Ames, CIA officer, arrested for espionage.
	6 May	Richard Miller, the FBI agent arrested for espionage on 3 October 1984, is released from prison.
	4 July	FBI opens a legal attache office in Moscow.
	1 August	The National Counterintelligence Center is established by Presidential Executive Order.
1995	23 June	Morris Cohen, 84, who also used the name Peter Kroger, died in a Moscow hospital. Cohen spied for the Soviet Union and was instrumental in relaying U.S. atomic bomb secrets to the Kremlin in the 1940s.
	12 September	George Kalaris, who succeeded James Angleton as chief of counterintelligence at CIA, dies.
	8 October	John Cairncross, 82, the so-called "fifth man" in the ring of spies recruited at Cambridge University in the 1930s to work for Moscow, died in Western England after a stroke. The other four spies were Kim Philby, Guy Burgess, Donald Maclean and Anthony Blunt.
1996	23 February	Robert Lipka, former National Security Agency clerk, is arrested by the FBI on espionage charges.

IMPORTANT DATES AND COUNTERINTELLIGENCE EVENTS

CLOSING THE 20TH CENTURY 1990-PRESENT

1996	27 February	Former Sgt Clayton Lonetree, the only US Marine ever convicted of espionage, is released from prison.
	1 March	The Commission on the Roles and Capabilities of the United States Intelligence Community—known as the Aspin-Brown Commission—released its final report entitled *Preparing for the 21st Century: An Appraisal of U.S. Intelligence.*
	14 June	President signed and forwarded to Congress the first Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, prepared by NACIC.
	24 September	Pavel Sudoplatov, a former senior KGB officer, who claimed to have engineered the stealing of the atomic bomb secrets from the United States, died.
	25 September	Robert C. Kim, a civilian computer expert at the Office of Naval Intelligence, is arrested for passing documents to a South Korean Embassy official.
	15 November	Alger Hiss died. He was the center of controversy over his espionage activities on behalf of the GRU for which he was never tried. Instead, he spent four years in prison for perjury when he lied to a grand jury in 1950.
	16 November	CIA officer Harold James Nicholson is arrested for spying for the Russians.
	18 November	John Vassall, a former British naval attaché, who admitted to spying for the KGB and sent to prison in 1962, died in London at age 71.
	7 December	Patrick and Daniel Worthing are arrested by the FBI. On April 18, 1997, Daniel Worthing became the first person in the US to be convicted under the Economic Espionage Act of 1996.
	18 December	Earl Edwin Pitts, an FBI agent, is arrested for spying for Russia.
1997	3 March	Harold James Nicholson plead guilty to espionage and was sentenced on 5 June 1997 to 23½ years in federal prison.
	30 April	Donald Ratcliffe, head of Far Eastern Operations for Litton Industries Inc., arrested by South Korean intelligence on charges of obtaining classified information.

IMPORTANT DATES AND COUNTERINTELLIGENCE EVENTS

CLOSING THE 20TH CENTURY 1990-PRESENT

1997	4 June	Kai-Lo Hsu, Technical Director of the Yeun Foong Paper Co. Ltd., in Taipei, and Chester S. Ho, a professor at the National Chiao Tung University, are arrested in Philadelphia on charges relating to an alleged plan to steal trade secrets from the pharmaceutical firm Bristol-Myers Squibb Company.
	5 June	Patrick Worthing convicted under Economic Espionage Act of 1996 for trying to sell PPG Industries trade secrets to Owens-Corning Fiberglass of Toledo, Ohio.
	10 June	Kelly Therese Warren, former U.S. Army clerk, arrested for espionage. She was the fifth person to be charged in connection with the Clyde Lee Conrad espionage ring as a result of a 10-year probe by the FBI and Army intelligence.
	23 June	Earl E. Pitts, former FBI agent, sentenced to 27 years in prison.
	11 July	Robert C. Kim, former Navy computer specialist, sentenced to nine years in prison for passing classified material to officials in South Korea.
	25 July	Donald Ratcliffe, the first American defense contractor to be arrested in South Korean on espionage charges, convicted and given a suspended two-year sentence.
	24 September	Ex-NSA employee Robert S. Lipka is sentenced to 18 years in prison and fined $10,000 for selling top-secret documents to the Soviet Union three decades ago.
	4 October	Theresa Squillacote, Kurt Stand, and James Michael Clark are arrested and charged with spying for East Germany and Russia in an espionage operation that began in 1972.
	3 November	Harold C. Worden, a retired Eastman Kodak manager, is sentenced to a year in prison and fined $30,000 for stealing formulas, drawings and blueprints from the company.
	8 December	Peter S. Lee, a nuclear physicist, pleaded guilty to willfully passing national defense information to Chinese scientists during a 1985 visit to China.

IMPORTANT DATES AND COUNTERINTELLIGENCE EVENTS

CLOSING THE 20TH CENTURY 1990-PRESENT

1998	8 January	Clyde Lee Conrad, a former US Army Sergeant who was convicted of treason in 1990, died in a German prison where he was serving a life sentence.
	26 January	Steven L. Davis pleaded guilty to federal charges that he stole and disclosed Gillette Company trade secrets. He was sentenced on 17 April 1998 to 27 months in prison.
	3 April	FBI arrests CIA employee Douglas Frederick Groat on charges of espionage.
	11 May	Israel officially acknowledged for the first time that Jonathan Pollard was an Israeli agent.
	3 June	James Clark, a one-time campus radical and former US Army paralegal, pleaded guilty to conspiracy to commit espionage.
	15 June	The French magazine Le Point reported that France systematically listens in on the telephone conversations and cable traffic of many businesses based in the United States and other nations.
	17 June	Department of Defense declassified its first reconnaissance satellite, which was launched shortly after the 1 May 1960 shoot-down of Francis Gary Powers' U-2 over the Soviet Union.
	27 July	CIA employee Douglas Frederick Groat pleads guilty to one count of attempted extortion after a plea agreement.
	28 July	FBI arrests Huang Dao Pei, a Chinese-born naturalized US citizen on charges he tried to steal trade secrets for a hepatitis C monitoring kit from Roche Diagnostics from 1992 to 1995 and sell it to China.
	1 August	Joel Barr, an American Communist and friend of Julius and Ethel Rosenberg, who barely eluded the FBI before he could be arrested for espionage in 1950, died of complications of diabetes in a hospital in Moscow.