DEPARTMENT OF DEFENSE

HOSTILE INTELLIGENCE THREAT
- U.S. TECHNOLOGY -

This publication outlines the hostile intelligence threat to U.S. industry and Western technology, including the operational capabilities of hostile intelligence services and their scientific and technological (S&T) targets. Current intelligence strategies used against the United States are described and sources of information providing countermeasures guidance are listed. Points of contact for security and counterintelligence assistance have also been included.

NOVEMBER 1988

ACKNOWLEDGMENT

This publication was prepared in the Office of the Assistant Deputy Under Secretary of Defense (Counterintelligence and Security) by Robert D. Davidson, United States Air Force Security Specialist Intern, from a variety of sources, which include:

– *Meeting the Espionage Challenge: A review of the United States Counterintelligence and Security Programs,* report of the Select Committee on Intelligence, United States Senate, October 1986.

– *A Report on Foreign Espionage in the United States,* United States Department of State, March 1987.

– *Soviet Acquisition of Militarily Significant Western Technology: An Update,* September 1985.

– *The Sentinels of Freedom, The American People and the Defense of the Nation's Secrets,* Federal Bureau of Investigation, April 1987.

This publication was developed with assistance provided by three other United States Air Force Security Specialist Interns- Greg Chavez, Susan Olsen, and Scott Wobbe. Special thanks go to them for their persistence in bringing this project to a successful conclusion and for their commitment to excellence.

Maynard C. Anderson
Assistant Deputy Under Secretary of Defense
(Counterintelligence and Security)

PREFACE

The hostile intelligence threat arrayed against the United States is pervasive and sobering and confronts the government and our nation's industry with increasingly serious challenges. The threat spans all types of intelligence operations to include traditional human espionage, the most sophisticated electronic devices, and technology transfers. Every kind of sensitive information is vulnerable, including classified government information, industry's emerging scientific and technological (S&T) breakthroughs and unclassified military related technical data.

Over the past two decades, the United States has increased reliance on the industrial sector for research, development, test and evaluation (RDT&E) of intricate components for major weapon systems, and command, control, communications and intelligence systems. This shift from government RDT&E to industrial RDT&E has also shifted the direction of hostile intelligence service collection efforts. Espionage cases over the past ten years (involving such industry personnel as Boyce, Bell, Schuler, Harper, and Cavanagh), and the discovery of a growth in incidents of illicit technology transfer, reflect this trend.

Hostile intelligence services depend to a large degree on their human collection networks throughout the world to satisfy their requirements for U.S. advanced technology. The agents who steal most of the U.S. classified information through espionage are not foreign nationals, legal or illegal, but Americans already employed in sensitive positions. These persons are recruited, or volunteer, to provide information to the hostile intelligence service.

The Western lead in many key technological areas has been reduced by a Soviet commitment of enormous resources to acquire open-source information, unclassified but proprietary information, and high technology equipment that the West has agreed not to export to the Soviet Bloc.

Hostile intelligence services also monitor many U.S. domestic telecommunications channels, including most satellite links and certain ground-to-ground transmissions. While the risk to military secrets from poor communications security is widely understood, the U.S. industrial community is also highly vulnerable.

Taken together, the damage to national security from espionage, technology theft and electronic surveillance amounts to a staggering loss of S&T information to hostile intelligence services. As an open society, the United States allows its' adversaries unfettered access to vast amounts of information that must be shared widely so that our political system functions democratically and the process of free scientific inquiry is most productive.

The United States must respond to this threat through a combination of the effective use of government counterintelligence operations to detect and neutralize hostile intelligence forces, and industrial security countermeasures.

SOURCES OF THREAT

Among foreign intelligence services, those of the Soviet Union represent by far the most significant intelligence threat in terms of size, ability and intent to act against U.S. industry. The activities of the Warsaw Pact and Cuban intelligence services are primarily significant to the degree that they support the objectives of the Soviets. The threat from intelligence activities by the People's Republic of China (PRC) is also significant.

Soviet Union

The principal elements that spearhead the Soviet intelligence services (S1S), the Committee for State Security (KGB) and Chief Directorate for Intelligence (GRU), are most often assigned to the United States under "official" cover at the Soviet Embassy in Washington D. C., the Soviet Consulate in San Francisco, and the Soviet Mission to the United Nations in New York City. The United Nations employs approximately 300 Soviet nationals as international civil servants. Approximately one-fourth of the Soviets in the Secretariat in New York are considered to be intelligence officers, and many others are co-optees who have been told to respond to KGB and GRU requests for assistance.

The openness of our society permits the Soviets to acquire much of the information their Military Industrial Commission (VPK) of the Presidium of the Council of Ministers has identified for collection through non-clandestine means. This collection is carried out through diplomatic activities, trade representatives, visitors, students, and through the open exploitation of readily available sources of desired information, such as public libraries and technical data banks.

Soviet intelligence has made extensive use of East-West exchange programs (EWEP). Soviet EWEP participants generally fall into two categories: 1) Soviet Exchange Scholars studying or conducting research at American colleges and universities; and 2) Soviet delegations, including Soviet scientists, businessmen, and scholars/academicians temporarily visiting the United States to attend various scientific, academic, business and cultural symposiums.

Tasking generally includes gathering S&T information as well as spotting and assessing potential recruits among American scientists and Soviet emigrees. The Soviet scientist, technician, or student visiting the United States is often in the best position to serve SIS interests simply by virtue of his or her expertise in a given field, and the freedom of movement and accessibility to information on American technology and technical personnel. While Soviet intelligence co-opts a significant number of legitimate scholars to act in an intelligence gathering capacity, the KGB and GRU also fill a number of these positions with their own personnel,

Finally, there are their American agents, who provide access to classified national security information and unclassified military related S&T information which is not accessible to the Soviets themselves. Most recent Soviet intelligence successes in penetrating the U.S. industry appear to originate from these "volunteers." Soviet intelligence continues to expend considerable manpower, time, and resources to spot, cultivate, and recruit Americans with access to classified or sensitive information–particularly overseas.

The Soviet methods used to acquire S&T information depend largely on the cost and risk involved. It is likely that increased controls on trade with the Soviets and on Soviet visitors and official personnel will cause changes in Soviet collection techniques. Thus, more use of clandestine methods and surrogate intelligence services to acquire technology is likely.

Soviet Use of Surrogate Intelligence Services

The intelligence services of Poland, East Germany, Czechoslovakia, Bulgaria, Hungary and Cuba act as surrogates for Soviet intelligence. While a member of the Warsaw Pact, Romania has looser ties to the Soviets in the intelligence arena. Thus, travel of Warsaw Pact and Cuban intelligence personnel is often clearly related to Soviet intelligence objectives.

Bulgaria

A substantial percentage of the approximately 84 Bulgarian officials in New York City and in the Bulgarian Embassy in Washington D.C. are considered to be known or suspected of affiliation with Bulgarian intelligence services (BIS). To further Bulgarian collection requirements, the BIS frequently exploits the roughly 1,000 annual Bulgarian visitors to the United States. The principal Bulgarian target has been embargoed technology.

Czechoslovakia

A significant number of the approximately 144 officials assigned by the Czechoslovakia Socialist Republic to diplomatic and commercial establishments in New York City; Charlotte, North Carolina; New Orleans, Louisiana; and the Czechoslovak Embassy in Washington D.C. are considered to be known or suspected of affiliation with the Czechoslovak intelligence service (CIS). The CIS have been aggressive in conducting intelligence operations in the United States, particularly in making contacts with U.S. citizens. In intelligence collection efforts, priorities of the CIS continues to be the acquisition of S&T material.

German Democratic Republic (GDR)

The East German intelligence services (EGIS) historically have used visiting illegals (posing as businessmen and students/scholars) in executing its intelligence operations. The central focus of the EGIS collection continues to be the acquisition of a broad variety of scientific and advanced dual-use technology.

Hungary

There are approximately 110 Hungarian officials stationed throughout establishments in New York City; the Hungarian Embassy in Washington D. C.; and small commercial offices in Chicago, Los Angeles, Newark, and Columbus, Ohio. The Hungarian intelligence service (HIS) is significantly represented among these officials and continues to concentrate on the S&T fields.

Poland

A significant percentage of the approximately 300 Polish officials currently assigned to the United States has been identified as known or suspected Polish intelligence officers. In conducting their intelligence operations, they have unquestionably used and exploited their freedom to travel within the United States to engage in espionage activities against the U.S. military and industrial sector.

Romania

There are approximately 72 official Romanian representatives in the United States, located predominately in New York City. Some of these 72 officials have known or suspected affiliation with the Romanian intelligence services (RIS). The Romanians in the United States do not concentrate as much of their intelligence efforts to the collection of highly sensitive S&T inforrration. However, they remain a threat as they continue to travel within the United States for intelligence purposes.

Cuba

The Government of Cuba (GOC) is represented in the United States by approximately 127 individuals at the Permanent Mission of Cuba to the United Nations in New York City and the Cuban Interests Section in Washington, D.C. This includes a significant percentage of officials with known or suspected affiliation with the Cuban intelligence services (CuIS). Cuban intelligence officers are in frequent contact with U.S. citizens, mainly to lobby against the U.S. trade embargo against Cuba.

People's Republic of China

The People's Republic of China (PRC) has several intelligence services whose personnel are represented among the approximately 1,500 Chinese diplomats

and commercial representatives located at some 70 PRC establishments and offices in the United States. They also have some access to the approximately 15,000 Chinese students and 10,000 individuals arriving in 2,700 delegations each year. PRC intelligence also seeks to exploit the large ethnic Chinese community. The PRC services concentrate primarily on S&T Information not approved for foreign release.

Other Countries

Because North Korea, Vietnam, and Nicaragua have only a limited official presence in the United States, their intelligence activities pose a lesser, but still significant threat to U.S. interests.

Many other countries–hostile, allied, friendly and neutral–engage in intelligence operations in the United States. While these activities cannot be ignored, they do not represent a comparable threat.

DUAL-USE EQUIPMENT AND TECHNOLOGY TARGETED BY HOSTILE INTELLIGENCE SERVICES

In order to improve the technical levels and performance of weapons and defense manufacturing equipment, hostile intelligence services seek to obtain the following military and dual-use hardware, blue-prints, product samples and test equipment:

MICROELECTRONICS

- Advanced Integrated Circuits
  - GaAs Devices
  - Memories
  - Microprocessors & Peripherals
  - Very-High Speed Integrated Circuit (VHSIC) Devices
- Automatic Integrated Circuit & Printed Circuit Board Testers
- Chemical Vapor Deposition (CVD) Equipment, Especially Metal-Organic CVD Systems
- Computer-Aided Design (CAD) Systems
- Integrated Optics
- Ion-Beam & Plasma Etchers
- Ion-Implantation Equipment
- Lithography Equipment, Especially Electronbeam, Ion-Beam, and X-Ray Systems
- Molecular Beam Epitaxy (MBE) Systems
- Semiconductors
  - III-V & II-VI Compounds
  - Heteroepitaxial Materials
  - Specialized Crystal Pullers
  - Quality Silicon for Very-Large Scale Integrated (VLSI) Circuits

COMPUTERS

- Array-Transform Processors
- Artificial Intelligence Systems
- Data Display Equipment
- High-Density Disk Storage Systems
- Internal Memories
- Software Development Systems
- Stand-Alone Mainframe Computers
- Supercomputers
- Superminicomputers

COMMAND, CONTROL, **COMMUNICATIONS,** AND INTELLIGENCE **(C3I)**

- C31 Software
- Computer Networking Systems
- Telecommunications
  - Fiber-Optics Transmission Systems
  - Digital Switching Systems
  - High-Speed Modems
  - Satellite Communications Systems
  - Terminal Displays

COMPUTER-INTEGRATED **DESIGN AND MANUFACTURING**

- Computer-Aided Design Software, Methods, and Equipment
- Computer-Aided Manufacturing (CAM) Software
- Computer Numerical Controls for Metalworking Machines
- Coordinate Measuring Machines
- Finite Element Analysis
- Flexible Manufacturing Systems (FMS)
- Plant Control Software
- Robotics

MATERIAL FABRICATION

- Metals and Alloys
- Composites
  - High-Strength Fibers & Filaments
  - Carbon-Carbon Manufacturing
- Ceramics
- Materials Processing
  - High Temperature Resistant Coatings
  - Isostatic Presses
  - Lasers for Surface Conditioning and Material Processing
  - Material Joining & Bonding Equipment
  - Nondestructive Test & Evaluation Equipment
  - Precision Shapers and Formers
  - Vacuum Furnaces, Including Those for Single Crystal Growth
- Fracture Mechanics

MISCELLANEOUS

- Gas Turbine Engines
- Large Floating Drydocks
- Space Launch Vehicles and Space Craft
- Navigation, Guidance and Control Technologies
- Nuclear Energy
- Directed Energy
- Microwave
- Sensors
- Underseas Systems
- Developments in Genetic Engineering
- Superplasticity

TYPES OF THREAT

The following are the legal and illegal methods by which an intelligence service may collect U.S. scientific and dual-use technology:

LEGAL

- Purchases
- Licenses (Justifications are revealing)
- Patents and Copyrights (Technical support data is detailed)
- Contracts, Bids and Proposals (Technology compromised when promoted for economic benefit)
- Joint Ventures and Coproduction Agreements (Significant information may be disclosed to foreign intelligence services using Soviet bloc commercial entities in the United States. These commercial establishments include the USSR's AMTORG and INTOURIST, the Polish-American Machinery Company (Polamco), and similiar East German, Czechoslovak and other East European entities. Altogether, nearly 70 U.S. chartered corporations, although owned by Warsaw Pact countries, function legally as U.S. corporations and thus are subject to few restrictions on acquiring technologies. However, these Warsaw Pact country owned corporations are subject to the same export restrictions as U.S. owned corporations. East Europeans employed by these firms are not subject to travel controls or notice requirements.)

. Purchase of Manufacturing Plants (Turnkey)
Technical Agreements

. Scientific Exchanges

- Student and Commercial Exchanges and Cultural Visitors (Some 2,000 Soviets come to the United States each year under the auspices of the Soviet Academy of Sciences, the Ministry of Trade, the State Committee for Foreign Economic Relations, and other Soviet agencies. Among their educational and cultural responsibilities, they also collect overt information from nondefense industries and classified and proprietary data in response to intelligence tasking on behalf of military research projects. The number of U.S. universities and institutes subject to focused Soviet efforts reportedly increased from 20 to 60 from the late 1970s to the early 1980s.)
- Scientific, Technical and Academic Conferences and Exhibits (Soviet trade or scientific representatives travel to California about four times a month in delegations ranging from two to ten people, supplementing the 41 person staff of the Soviet San Francisco Consulate. It is reasonable to assume that 30 to 40 percent of the personnel in a Soviet visiting delegation

are intelligence officers and/or co-optees. Thus, the Soviets are able to target more intensively the 1,500 high-technology companies in the "Silicon Valley," which constitutes the largest collection of electronics and computer manufacturers in the United *States.)*

- Industrial Tours
- Publications (Scientific, Commercial, Textbooks, Sales Brochures, Congressional)
- Immigration
- Captured Weapons
- Loose Talk

ILLEGAL

The illegal hostile intelligence threat can be divided into two categories; the human side and the wide array of technical collection operations.

• Human Intelligence Threat (HUMINT)

The HUMINT dimension begins with the trained intelligence officer dispatched under official or nonofficial cover to operate abroad, Intelligence officers are tasked to recruit U.S. military, government, and contractor personnel in addition to co-opting other members of their own government and citizenry for particular assignments. Persons with direct or even indirect access to sensitive or classified information are the prime targets of any foreign intelligence service operating against the United States. In general, the hostile intelligence HUMINT operations fall into the following categories: Legals, Illegals, Co-optees, and Agents as defined under Definitions.

The possibility of being targeted for HUMINT exploitation increases outside of the United States where foreign intelligence services are less vulnerable to U.S. counterintelligence detection. Their operations may be bolder since the target, an American civilian or military member, is on unfamiliar ground and may be more easily approached, entrapped, and exploited.

• Recruitment Approaches

Hostile intelligence services begin the agent recruitment process by scrupulously collecting information on persons who are connected to industry, RDT&E laboratories, government institution staffs, military bases, and design organizations,

A candidate for recruitment usually fulfills the following criteria:

– They must be in a position to provide information of real use to the hostile intelligence service, either to steal or copy S&T information, to communicate secret information by word of mouth, or to recruit new agents.

– There must exist motives by means of which an individual can be recruited:
  – Financial Consideration/Greed (Transcends all other motives)
  – Revenge/Disaffection
  – Blackmail/Hostage Situations (Used in USSR but very infrequently in U. S.)
  – Appeal to Emigres National Pride
  – Exploitation of an Emotional Involvement
  – False Flag Approaches
  – Exploitation of an American's Naivete
  – Sex
  – Ideology (Not the motivation it once was. Soviets now concentrate on sympathy for "persecuted"' elements of American society)

After the selection of a candidate for recruitment, the first stage, tracing and cultivating, commences. Details are collected about the candidate, details which may be obtained through reference, books, telephone directories, the press, and other recruited agents. Further definition of motives which will be used in the actual recruitment of the person are cultivated and weaknesses are exacerbated.

After the cultivation stage, overt contact is established with the candidate under the guise of an official meeting. After the acquaintanceship has ripened and official meetings evolve into personal meetings, the developmental *stage* begins. The developmental stage cements the relationship and encourages loyalty to it. The hostile intelligence officer may then, through friendly persuasion, ask for a very innocent and insignificant favor from the candidate and pay him generously for it, thus placing the candidate in a position of obligation. During this stage the future agent becomes accustomed to being asked favors and fulfilling them accurately. The future agent's ambitions, financial and work problems, hobbies, etc., are continuously assessed by an intelligence team to exacerbate weaknesses. The future agent's professional, social, and private personalities are soon stripped away.

By degrees the tasks become more complicated, but the payment for them grows equally, In many cases the actual recruitment proposal is never made, as the candidate gradually becomes an agent of the hostile intelligence service without fully realizing it. He may consider that he is simply doing his business and doing favors for a good friend. I-he candidate will find that all means of extricating himself have been cut off, and that he is deeply ensnared in espionage work.

The final stage is the recruitment stage, where the relationship moves from overt to covert. The tasks become more serious but the payments for them

gradually decreases, This is done on the pretext of the agent's own security. In actuality, the agent is no longer in a position to negotiate fees for his information, he is trapped.

There is a more dangerous type of agent than the person who has been ensnared in espionage work; this agent is the volunteer who walks into a foreign embassy and asks to be recruited. Volunteers who are "warmly welcomed" do not take into consideration the fact that they are despised by hostile intelligence agents. A quote from a former Soviet GRU intelligence officer who defected to the West offers the following insight:

> "The Soviet operational officer, having seen a great deal of the ugly face of communism, very frequently feels the utmost repulsion to those who sell themselves to it willingly. And when a GRU or KGB officer decides to break with his criminal organization, something which fortunately happens quite often, the first thing he will do is try to expose the hated volunteer."

- **Technical Collection Operations**

Hostile intelligence services use the full range of intelligence gathering technologies, to include the interception of communications, electronic surveillance, collection of emanations from equipment, penetration of computer systems, photoreconnaissance, and collection of S&T information from the United States.

– SIGNALS INTELLIGENCE (SIGINT): The Soviet interception of U.S. communications represents a significant threat to the United States. By monitoring telephones and radio transmissions, Soviet technical service groups can obtain S&T information from a variety of locations and a fleet of intelligence collection vessels and merchant ships that operate worldwide - including off both coasts of the United States.

Today the discipline of SIGINT also encompasses the collection of electronic signals of all kinds, such as radar and equipment emanations, telemetry from weapons testing, and microwave transmissions sent via microwave towers and satellites.

SIGINT also includes the penetration of computer systems. Over the past decade, the Soviets have acquired over 300 different types of U.S. and other Western computer hardware and software, which has enabled them to develop the technical ability to penetrate at least some of the U.S. automated systems.

– IMAGERY: The final category of technical intelligence collection is photographic or imagery intelligence–collection by means of overhead satellites, commercial aircraft, or hand held devices against industrial RDT&E grounds or military targets.

COUNTERING THE THREAT

In order to assist the industrial sector in countering the hostile intelligence threat and in protecting classified government information along with industry's emerging S&T breakthroughs, the Office of the Deputy Under Secretary Defense (Policy) provides valuable guidance in DoD 5220.22-M, "Industrial Security Manual (ISM) for Safeguarding Classified Information," September 1987. The ISM is available through the contractor's local Defense Investigative Service (DIS) cognizant security office. In addition to the ISM, further guidance is provided in the following supplements:

- DoD 5220.22-S-1, "COMSEC Supplement to Industrial Security Manual for Safeguarding Classified Information," March 1988.
- DoD 5220.22-S-2, "Marking Supplement to Industrial Security Manual for Safeguarding Classified Information," September 1987.
- DoD 5220.22-C, "Carrier Supplement to Industrial Security Manual for Safeguarding Classified Information," October 1986.

Provided the contractor has a contract (DD Form 254) specifying access to classified COMSEC material and a facility clearance of SECRET or above, the following TEMPEST guidance is also available from the contractor's local DIS cognizant security office:

- NACSI 5004, National COMSEC Instruction, TEMPEST Countermeasures for Facilities Within the United States(U)," January 1984.
- NACSI5005, National COMSEC Instruction, TEMPEST Countermeasures for Facilities Outside the United States(U)," January 1984.

The Naval Publications and Forms Center (NPFC) and National Technical Information Service (NTIS) have the following directives and regulations available for additional guidance:

• Technology Control

- DoD Directive 5230,24, "Distribution Statements on Technical Documents," March 18, 1987. (NPFC)
- DoD Directive 5230.25, "Withholding of Unclassified Technical Data trom Public Release, " November 6, 1984.(NPFC)

– DoD 5230.25-PH, "Control of Unclassified Technical Data With Military or Space Application, " May 1985. (NTIS)

– DoD 3200.12-R-4, "Domestic Technology Transfer Program Regulation (USDA)," April 1985. (NTIS)

– DoD 2040.2(D), "International Transfer of Technology, Goods, Services, and Munitions, " Change 1, January 17, 1984. (NPFC)

. Communication Security (COMSEC)

– DoD 5210.74, "Security of Defense Contractor Communications, " June 26, 1985. (NPFC)

written requests for individual copies should be submitted to:

NPFC:

Commanding Officer
A'[TN: Code 301
Naval Publications & Forms Center
5801 Tabor Avenue
Philadelphia, PA 19120-7099

Commercial Telephone:
(215) 697-3321 or 2179

NTIS:

National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

All requests must include personal or company name and complete mailing address (street address or P.O. Box number, city, state and zip code).

The Department of Defense Security Institute (DoDSI) also provides the following security awareness publications upon request:

- (SAM) Soviet Acquisition of Military Significant Western Technology: An Update. September 1985. Detailed description of Soviet efforts to obtain Western high technology, by fair and foul means. Includes details on types of technology sought and Defense contractor firms, listed by name, which the Soviets have targeted.

- (REC) Recent Espionage Cases: Summaries and Sources. Updated periodically. Forty-three cases, 1979 to 1986, "Thumb-nail" summaries and open source citations.

- (HIT) Hostile Intelligence Threat to U.S. Industry: An Assesment for the Defense Industrial Security Program. January 1981. By DODSI Staff.

– (FTB) Foreign Travel Briefing. 1981. Script of briefing designed for cleared employee's traveling to communist-controlled countries. Outlines methods used by hostile intelligence services and precautions against them.

- (TAS) Training Aids for Security Education. Updated periodically. Catalog of audiovisual and printed material of interest to security educators, Instructions for ordering.

– Back issues of DoDSI Security Awareness Bulletins are also available, For a complete and updated list of back issues, reference a current copy of the Security Awareness Bulletin or write DoDSI at:

Department of Defense Security Institute
ATTN: Security Awareness Division
c/o DGSC, Richmond, Virginia 23297-5091

When ordering the above publications from DoDSI, please include the codes located before the publication title. Reproduction of publications is authorized unless otherwise specified, Please enclose a self-addressed mailing label (no postage required) and include your nine digit Zip Code.

REPORTING ATTEMPTED CONTACTS

If an individual has contacts with representatives from the Soviet Union, Warsaw Pact countries, Cuba, People's Republic of China, or other designated countries, there are a number of defensive steps that can be taken. The most important step is to report all such contacts (official, work-related, social, and professional) to a Security Officer who can monitor the contacts to protect the employee's record.

The Security Officer should be recognized as an ally and not an adversary. His job is to minimize damage that results from the loss of sensitive information, protect employees from getting ensnarled in situations involving hostile intelligence services, and to extricate them when necessary, This service cannot be rendered if the employee remains silent, It is much better for an employee to reveal a suspected relationship voluntarily than have it come to light in the course of an investigation. In sum, if an employee becomes involved in a compromising situation, the sooner he consults his Security officer, the better for all concerned: the employee, the employer, and the United States,

In situations where an employee cannot or, for some reason, does not want to contact his Security officer, the FBI can also be contacted. In the United States, the FBI is as close as the nearest telephone. Abroad, the nearest U.S. diplomatic establishment can arrange to put an employee in touch with

appropriate U.S. Government security officials. Any attempt by untrained or uninformed persons to take on hostile intelligence approaches single-handedly could result not only in personal disaster, but may also interfere with current counterintelligence efforts.

In addition to analyzing reported hostile intelligence approaches and proposing courses of action, the FBI also provides a Defense Counterintelligence Awareness (DECA) program which informs contractor employees about current signs and techniques of local recruitment attempts. The purpose of the DECA briefing is to sensitize the contractor employees to the vulnerabilities of having access to classified and sensitive S&T information.

The following agencies provide security and counterintelligence assistance to counter the hostile intelligence threat:

- PROGRAM MANAGER
  Telephone:
- INSTALLATION SECURITY OFFICE
  Telephone:
- LOCAL DIS COGNIZANT SECURITY OFFICE
  (Industrial Security Specialist)
  Telephone:
  Address:
- APPLICABLE LOCAL MILITARY SERVICE COUNTERINTELLIGENCE ORGANIZATIONS:
  - U.S. AIR FORCE OFFICE SPECIAL INVESTIGATIONS (0S1)
    Telephone:
  - U.S. ARMY INTELLIGENCE SECURITY COMMAND (INSCOM)
    Telephone: I-800-CALL-SPY
  - U.S. NAVAL INVESTIGATIVE SERVICE (NIS)
    Telephone:
- LOCAL FBI OFFICE
  Telephone:
- Personnel with information of a positive counterintelligence nature may also contact the DEFENSE INTELLIGENCE AGENCY (DIA):
  - COMMERCIAL: (202) 695-0361
  - AUTOVON: 225-0361
  - SECURE: (AUTOSEVOCOM) 2573
  - SECURE: (GREY LINE) 6132

Where appropriate, arrangements can be made to ensure caller anonymity.

DEFINITIONS

AGENT:

An American or third-country national recruited for current operational purposes or, in some cases as "sleepers" to be activated at a later date.

CLASSIFIED DEFENSE INFORMATION:

Official information requiring protection in the interest of national defense, classified TOP SECRET, SECRET, or CONFIDENTIAL according to DoD 5200.7-R, "Information Security Program Regulation," or designated Sensitive Compartmented Information (SCI) according to DoD TS-5 105.2 1-M-2 or DoD TS-51 05.21 -M-3

CONTACT:

Any form of meeting, association, or communication; in person, by radio, telephone, letter or other means, regardless of who initiated the contact or whether it was for social, official, private, or other reasons with a citizen or entity of a communist, communist-controlled, or designated country. A contact has occurred even if no official information was discussed or requested.

CONTROLLED INFORMATION:

That information which bears a distribution limitation statement from DoD Directive 5230.24, "Distribution Statements on Technical Documents" or that information which is being marked "For Official Use Only" in accordance with Chapter IV of DoD 5400.7-R, "DoD Freedom of Information Act Program."

CO-OPTEE:

Foreign official or visitor tasked to do particular tasks, such as spotting potential recruits or servicing drops. Many diplomatic officials are co-opted, as are many official visitors and emigres.

COUNTERINTELLIGENCE:

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities excluding personnel, physical, document, and communications security programs.

COUNTERINTELLIGENCE INVESTIGATION:

Includes inquiries and other activites undertaken to determine whether a particular person is acting for or on behalf of a foreign power for the purpose

of espionage or other intelligence activites, **sabotage, assassinations, international terrorist activites, and actions to neutral ize such acts.**

CRIMINAL SUBVERSION:

Criminal Subversion is defined in 18 U.S.C. 2387 as inciting military or civilian personnel of the Department of Defense to violate laws, disobey lawful orders or regulations, or disrupt military activities, with the willfull intent thereby to interfere with, or impair the loyalty, morale, or discipline of the military forces of the the United States.

DELIBERATE COMPROMISE OF CLASSIFIED INFORMATION:

Instances in which classified defense information is or could be compromised as a result of willful disclosure to an unauthorized person.

ENTITY:

Any embassy, consulate, trade, press, airline, cultural, tourist, or business office, or any organization representing a communist, communist-controlled, or designated country.

ESPIONAGE:

As set forth in 18 U.S.C. 792-798, in general:

a. Espionage is the act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent or reason to believe that the information may be used to the injury of the United States or to the advantage of any foreign nation. The offense of espionage applies in time of war or peace.

b. The statute makes it an offense to gather, with the requisite intent or belief, national defense information, by going upon, entering, flying over, or obtaining access by any means to any installation or place used by the United States in connection with national defense. The method of gathering information is immaterial.

c. Anyone who lawfully or unlawfully is entrusted with or otherwise has possession of, access to, or control over information about national defense which he or she has reason to believe could be used against the United States or to the advantage of any foreign nation, and willfully communicates or transmits, or attempts to communicate or transmit, such information to any person not entitled to receive it, is guilty of espionage.

d. Anyone entrusted with or having lawful possession or control of information pertaining to the national defense, who through gross

negligence permits the same to be lost, stolen, abstracted, destroyed, removed from its proper place of custody, or delivered to anyone in violation of this trust, is guilty of espionage.

e. If two or more persons conspire to commit and one of them commits an overt act in furtherance of such conspiracy, all members of the conspiracy may be punished for violation of the Espionage Act.

ILLEGALS:

Trained intelligence officers sent abroad, often with false identities, who maintain no overt contact with their government.

LEGALS:

Operations which are conducted by intelligence officers under official/diplomatic cover. The term does not mean lawful because case officers recruit and handle espionage agents.