If you have issues viewing or accessing this file contact us at NCJRS.gov.

Johnson/NCJRS
MF-1

U.S. Department of Justice

A Guide For Department of Justice Employees on the Threat from Hostile Intelligence Services

105809

Foreword

On November 1, 1985, President Ronald Reagan signed a National Security Decision Directive entitled "Reporting Hostile Contacts and Security Awareness." The United States Department of Justice and other Federal agencies were ordered to create and maintain a formal security awareness program to alert Federal employees of the threat by hostile foreign intelligence services against sensitive, proprietary, and classified national security information. In addition, all entities were required to establish a method for reporting an employee's contact with nationals of certain foreign countries.

As part of this Department's plan to promote security, I asked FBI Director William H. Webster to have a booklet prepared on security awareness for use by all employees of the Department of Justice. I ask that all of you read this booklet, as our security depends heavily on enlightened and supportive employees.

Edwin Meese III
Attorney General

105809

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~copyrighted~~ material has been granted by
Public Domain
U.S. Department of Justice
to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~copyright~~ owner.

INTRODUCTION

Recently, in a rural area just outside a major U.S. city, an individual parked his car on the roadside near a telephone pole. Although it was nighttime, the man had no difficulty finding the object of his drive in the country. He retrieved a rock and quickly drove from the area.

The rock was peculiar—it was hollow and crammed with twenty-dollar bills. The man, who was employed by the U.S. Government, was acting as an agent of the Soviet Intelligence services, and the payment was for services rendered. Included with the money were written instructions detailing future spy missions for the agent.

Fortunately, in this case the American was acting on behalf of the FBI as a "double agent" in a foreign counterintelligence operation. This type of operation is one of several tools used by the FBI to monitor and neutralize foreign espionage efforts in the United States.

The above episode was just one incident of many in the effort to detect and prevent espionage and other clandestine intelligence activities in the United States. It is true that major espionage cases often receive front-page coverage. For the most part, however, the conflict between American counterintelligence forces and hostile foreign intelligence services remains "unseen" to the public and most Federal employees.

This pamphlet has been written to shed some light on the targets and strategies of hostile intelligence services. By itself, the FBI cannot be successful in this conflict. To achieve success, the support and often the assistance of informed Department of Justice employees, particularly those who have access to classified information, must also be enlisted.

Espionage is the illegal gathering, through clandestine means, of information or material affecting national security. As described in Federal law, espionage is the gathering of information or material relating to the national defense and/or delivering, transmitting or communicating it to any person not entitled to receive it or to any foreign government with the intent or reason to believe that it is to be used toward the injury of the United States or to the advantage of a foreign nation. Such activities are proscribed by the United States Code, Title 18, Chapter 37.

The intelligence data that may be the target of espionage activities can take many forms. To the untrained observer the targeted data can be of obvious importance or may be, just as readily, seemingly innocuous. It can be technological, political, scientific, economic, sociological, geographical, and even personal information on individuals, particularly those with current or potential access to information of intelligence value. Of particular importance to a foreign intelligence service are the identification of what constitutes our vital political, economic, and military intentions, and the theft of America's military and scientific secrets. The principal repositories of such data are the United States Government and industries holding Government contracts relating to national defense.

To protect the national security from damage caused by the unauthorized disclosure of sensitive, strategic information, the Executive Branch of the United States Government has established a system whereby such vital information is

"classified." There are three levels of classification, and the basis for each level of classification is the degree to which the unauthorized disclosure of information would damage the national defense or foreign relations which constitutes the national security of the United States.

Based upon this system, the information which is granted the highest degree of protection is classified "*TOP SECRET.*" The *unauthorized disclosure* of such information which *reasonably could be expected to cause "exceptionally grave" damage* to the national security. Exceptional damage would entail disruption of foreign relations vitally affecting the national security, the compromise of vital national defense plans or complex cryptographic and communications intelligence systems, or the disclosure of scientific or technical developments vital to the national security. "Top Secret" material warrants maximum protection.

Unauthorized disclosure of information which *reasonably could be expected to cause "serious" damage* to national security is classified "*SECRET.*" Examples of serious damage are the disruption of foreign relations significantly damaging to the national security, disclosure of significant scientific or technological developments relating to national security, or the exposure of significant military plans or intelligence operations. "Secret" material also requires a substantial degree of protection.

The *unauthorized disclosure* of information which *reasonably could be expected to cause damage* to the national security is classified as "*Confidential.*" "Confidential" is applied to information which requires some protection and is the lowest level of classification.

Classified data of all levels must be maintained and protected in a special prescribed manner. Only Government employees and persons in the private sector who have appropriate security clearances and a "need-to-know" may view classified information. Controls are mandated for the accessibility, reproduction, transmittal, storage, and destruction of classified information to provide adequate safeguards.

The classification system is by no means a random or frivolous tool. Its purpose is the well-being and safety of the United States of America—the national security. It is judiciously and carefully applied. Within the United States Government there are only a limited number of specifically designated officials of the Executive Branch, in offices concerned with national security, who have the authority to classify documents. Material is carefully reviewed before being classified. If a document is unnecessarily classified or overclassified, the official responsible for the inappropriate classification may be subject to administrative action. If a document carries the label "Top Secret," "Secret," or "Confidential," one can be certain that it contains material vital to the national security. Such material should be handled and safeguarded with the greatest care.

The protection of classified information—preventing the unauthorized disclosure of certain information—may seem to have lost importance in this age of "leaks" and exposes in the press. Indeed, in some cases, individuals have actually achieved a degree of fame and glamour as a result of their unauthorized disclosure of classified information. They are viewed as heroes by many people for their wholesale unveiling of classified information. Barely a week goes by without a book being published, a newspaper appearing, or a television program

broadcast which includes, or appears to include, some leaked, classified information.

Perhaps more so than at any time in our history, we have entered an age of "open government"—an age in which a flood of information flows freely from sources which were at one time closely safeguarded. In this atmosphere of openness, a person could conclude that there is no need for security, no need of secrecy. This is simply not true. The classification system was created for the most compelling of reasons—the preservation of national security. The system is designed so that information not requiring protection may be disclosed. On the other hand, it is designed to assure that information vital to America's security is not scattered about the countryside. As an individual who has access to sensitive information, it is your responsibility to comply with and respect this system and to uphold your responsibility in safeguarding America's Top Secret, Secret, and Confidential information.

THE THREAT

Intelligence collection—the world of espionage and counterespionage—is a popular subject of fiction. It has been the topic of innumerable books, short stories, television serials, and movies. The role of the spy or the "secret agent" has become so sensationalized and exaggerated that it is easy to think that spies exist only in the minds of fiction writers, or that spying belongs in the same category as science fiction. Do not believe it!

Spies do exist, and several hundred spies, or "intelligence officers" as they are officially known, who are affiliated with what the FBI terms the "hostile intelligence services," now operate within the United States. These intelligence officers in turn operate "agents." The bulk of these spies have been dispatched by the Soviet Union, but the USSR's allied nations in Eastern Europe, as well as Cuba and other nations, also operate officers and agents within the United States.

The main objective of the hostile services is the systematic collection of information. The most prized item is, of course, classified U.S. Government material. Unclassified material can also be of inestimable value. Increasingly, advanced U.S. technology—much of which is barred from export to the Soviet Union, Soviet-bloc countries, Cuba, and the People's Republic of China—has become a major intelligence target.

Within the past decade, the number of intelligence officers pursuing these targets has swollen. Since 1972, the number of communist country officials assigned to the United States has increased by over 100 percent. It has been the experience of the FBI, confirmed by the experience of counterintelligence services of our allies, that roughly one out of three communist country officials is an intelligence officer—in plain language, they are spies.

Furthermore, the number of business representatives, scholars, and similar visitors from these countries has more than doubled in recent years. A large number of these individuals are also working for, or on behalf of, their respective intelligence services, thus greatly increasing the potential for espionage operations aimed at the general population and especially at Federal workers who come in contact with classified or restricted information.

Stark evidence of the effectiveness of the Soviet KGB (Committee for State Security) and other hostile intelligence services, and the threat posed by them to the United States, was exemplified in several recent espionage cases successfully developed by the FBI. The most damaging of these cases include:

- in late 1980, Henry David Barnett, a former CIA employee who tried to regain a position with the U.S. Intelligence Community, admitted that he had attempted to become a "mole" (i.e., a deep penetration agent) at the behest of the KGB, and had already sold CIA secrets to the Soviets;

- in 1981, Joseph George Helmich pled guilty to charges of espionage, after admitting he had sold to the Soviets, in the early 1960s, a large amount of information relating to a "Top Secret" United States crypto system which he obtained while in military service;

- in late 1981, an American citizen, William Holden Bell, and a Polish intelligence officer were arrested and convicted of espionage, after a large amount and variety of military-related technology was passed to Warsaw and, presumably, to Moscow;

- in 1985, John Anthony Walker, Jr., Michael Lange Walker, and Arther James Walker were arrested on espionage charges for their roles in obtaining and passing classified information to the Soviet Union;

- and also in 1985, retired CIA analyst Lawrence Wu-Tai Chin was arrested for giving classified information throughout much of his Government career, to the People's Republic of China.

In all of these cases, enormous damage was done to United States national security interests. For instance, the Central Intelligence Agency concluded that as a result of the Bell operation, the Polish and Soviet Governments would save "hundreds of millions of dollars in research and development efforts by permitting them to implement proven designs developed by the United States and be fielding operational counterpart systems in a much shorter period of time."

HOSTILE INTELLIGENCE SERVICES STRATEGY

In their task of gathering intelligence information, the intelligence services have a large array of tools. Satellites gather photographic data. Aircraft and sea vessels gather electronic intelligence. But a further source of data, and potentially the most valuable to a hostile nation, is the so-called "human source," i.e., the spy.

Probably the greatest achievement of an intelligence organization is the placement or recruitment of an agent in a sensitive position in a national defense or intelligence element of an opposing government. In addition, the penetration of private institutions involved in sensitive national defense-related research and development work can be of great value. Americans who have been recruited by

hostile intelligence services can also be used to serve as middlemen to acquire technology that has been embargoed from export to the Soviet Union, Soviet-bloc countries, Cuba, and the People's Republic of China. Even if an American does not have access to classified material or embargoed technology, he can be used as a so-called "spotter," who can supply personal data (perhaps unwittingly) about Americans who *do* have access to targeted material.

Therefore, the central mission of hostile intelligence service officers in the United States is the assessment and recruitment of Americans as agents. To this end, intelligence officers and their agents are constantly in contact with Americans and are evaluating them as potential recruitment targets. If an American appears to have potential for development as an agent, several different techniques or approaches may be used to recruit him. The following techniques may be used against a Department of Justice employee.

Financial Consideration/Greed

The man appeared to be quite successful—he held a job as an engineer with a top defense-related United States firm and, on the surface, was a model citizen. This was not the case, however, for he was in deep financial trouble. But there was a way out of his difficulties. He had recently been befriended by an East European businessman who, upon hearing of the engineer's difficulties, offered monetary assistance. The price would be small—merely supply the businessman with unclassified technical data from the engineer's firm, which he did.

However, even by supplying unclassified data, the engineer had compromised himself. Eventually, his "friend" requested classified information, and the engineer continued to fulfill the requests of the East European.

Needless to say, the East European "businessman" was no businessman, but a professional intelligence officer using his business association as a "cover" for clandestine intelligence collection. The engineer had become entangled in a full-fledged espionage operation. He was provided with concealment devices in which to hide stolen documents, executed clandestine meetings overseas and, before being arrested by the FBI, was paid in excess of $100,000 for his labors.

Of the various tactics used by spies, those geared to exploit an American's material needs are by far the most common and the most effective. Many Soviet and other communist agents believe that Americans, as capitalists, are hopeless materialists and can be swayed by greed. Usually, an intelligence officer will initially solicit innocuous material, responding with gifts or small sums of money, and then gradually attempt to acquire more sensitive information with larger payments following.

Blackmail/Hostage Situations

A U.S. Government employee, while traveling in the Soviet Union, was approached by an attractive woman. The exchange of conversation and the flow of vodka created an atmosphere which led the American to venture the proposition, "I suppose it's quite obvious that this representative of a 'decadent West-

ern society' would like to make love to you." His proposition was quickly, perhaps too quickly, accepted.

The American did not realize that the woman was a KGB agent, and that the ensuing events of the evening were being filmed by the KGB. Little did he realize that hostile intelligence services use blackmail overseas, and that he had become involved in a classic, compromise situation. The situation left him vulnerable to a blackmail attempt by the KGB.

Luckily, the American blunted the threat of any KGB coercion by revealing the full details of his unfortunate encounter to Federal authorities upon his return to the United States.

Hostile intelligence services can play rough in their drive to compromise and recruit U.S. citizens when Americans are visiting communist countries. Attempts at compromising Americans, through sex, drugs, and trumped-up arrests, while they are touring the Soviet Union and other East European countries, are not uncommon. At the same time, it should be emphasized that this approach is seldom, if ever, employed within the United States (although knowledge of any personal vulnerabilities of Americans is sought in the United States for exploitation abroad).

Another tactic employed by the hostile intelligence services is the exploitation of hostage situations. If a foreign intelligence service learns that a targeted individual has relatives in Eastern Europe, the USSR, Cuba, or the People's Republic of China, the individual is regarded as being in a potentially vulnerable position. First will come gentle persuasion. An intelligence officer may produce "letters" from relatives calling for the American to "cooperate." If that doesn't work, the intelligence officer may suggest that harsh measures could be applied to the relatives. There is no easy answer to the American who finds himself approached in this manner, because the ability of the hostile intelligence service to apply pressure through the target's family is unquestionable.

Appeal to National Pride

An employee of a leading computer firm who was of East European descent was invited to tour his native country. Upon arriving in Eastern Europe, he was treated graciously by government officials and was provided with a personal "guide" to accompany him on the tour. The "guide" was in reality an operative of an East European intelligence service, whose assignment was to assess the individual's potential for recruitment as an agent. A year after the computer specialist had returned to the United States, he was contacted by an official from his native country. The official arranged a luncheon date with the specialist. At lunch, he attempted to elicit computer-related information. The inducement used was an appeal to the sense of pride in the specialist's native land.

This case had a positive outcome. Recognizing the irregularity of this contact, the computer specialist immediately contacted the FBI. This was fortuitous, for the "official" was, in actuality, a full-fledged intelligence officer.

This particular recruitment approach is favored by intelligence officers of the Eastern European and Soviet-bloc countries and is aimed at emigrants from

those countries. In some cases, unwitting emigrants have been goaded into cooperation by East European "diplomats." They did not realize that the "diplomats" were intelligence officers and that the information supplied to the intelligence officers was not intended to help their native land, but was actually headed for Moscow.

Exploitation of an Emotional Involvement

A recent espionage case revolved around a U.S. Government employee who supplied classified documents to a foreign agent. What made this case unusual was the fact that the American received no monetary payment for his treachery. He became ensnared in espionage because he wished to be reunited with his lover, who had become stranded in a communist country. An agent of that country, recognizing the American's vulnerability, was only too willing to come to his assistance—for a price. In return for his services, the communist agent demanded classified data. The American complied and soon became reunited with his lover, but not for long. His activities were uncovered by the FBI, and he was eventually convicted and sentenced to 15 years in prison.

"False Flag" Approaches

In another maneuver, a hostile intelligence officer misrepresents himself as a citizen of a country friendly to the United States. This is called a "false flag approach." Thus, a targeted American may be duped into handing over sensitive information by being led to believe that he is aiding an ally of the United States.

In a variation of this tactic, an intelligence officer or a hostile intelligence service agent poses as a representative of a noncommunist country or entity, toward which a targeted American is particularly sympathetic.

This approach was used in a case which occurred during the mid-1970s. An American of Armenian extraction was approached by another Armenian who said that he was a "distant relative." The relative claimed he was working for Armenia, with the assistance of the Soviet Union, in a drive to reclaim lost Armenian lands from Turkey. The distant relative was, in actuality, a KGB agent who eventually duped the unsuspecting immigrant into giving him classified information.

Approaches Based on Ideology

If a hostile intelligence service officer or agent believes that an individual has communist sympathies, he may make an appeal for information based on ideology. This type of approach is now less frequently observed than in the 1950s and 1960s. A "pitch" for information may also be geared to take advantage of an American's desire for international harmony and world peace. An intelligence officer can also exploit an American's concern for a single issue, such as nuclear disarmament, by claiming to have a similar concern, and thus ingratiate himself

with the American.

In a case which occurred in the mid-1970s, an American scholar in Europe who already was sympathetic toward the Soviet Bloc was approached by a hostile intelligence service. The student eventually agreed to cooperate with the service in working for "world peace and harmony." He became an agent of a communist country.

The student returned to the United States and, at the direction of his handlers, attempted to gain employment with the U.S. Government in a position which would give him access to highly sensitive data. But his identity as an agent was detected, and he was effectively neutralized.

In a more recent and famous case, retired CIA analyst Lawrence Wu-Tai Chin was arrested and convicted of passing classified information to his native China. Chin said he believed the information would foster a better understanding of the United States by the Chinese.

Exploitation of an American's Naivete

This approach may be used against an impressionable individual. A common tactic for a hostile intelligence officer is to exploit traditional American beliefs, such as freedom of speech or the conviction that scientific advancements should be allowed to benefit all mankind, in an attempt to elicit information.

An intelligence officer or agent in the role of a "student" or "researcher" may urge an American "colleague" that knowledge has no political boundaries or that the field of science is beyond politics. In the interests of scholarship and science, the American is encouraged to exchange the results of his research with a fellow member of the international community of scientists.

Revenge/Disaffection with Job

An element which has been at the center of many espionage cases is revenge. Disgruntled employees may seek a quick way to wreak vengeance and be paid as part of the bargain by selling valuable information to a hostile intelligence service. Needless to say, if an intelligence officer determines that a targeted American is dissatisfied with his job, the spy will zero in on this discontent.

The best example of revenge in action occurred in the William Kampiles case. While employed by the CIA, Kampiles had been told by his superiors that his chances of advancement were minimal due to his poor work performance. He then resigned in a huff from the CIA and while departing, stole a highly sensitive and valuable classified document, which he sold to the Soviets. Certainly, Kampiles gained some measure of revenge against the CIA, but in the process did grave harm to the National Security of the United States. As a result of his impulsive gesture, he was sentenced to 40 years in a Federal penitentiary.

COUNTERING THE THREAT

There is a common notion among Americans that the KGB is staffed with crude Russians, who have bushy eyebrows, wear baggy suits, and speak with thick accents. Nothing could be further from the truth—the KGB is an elite organization composed of individuals from the upper strata of Soviet society, generally well-educated and sophisticated. An important first step toward countering the spy threat is not to underestimate the capabilities of the KGB or, for that matter, any of the hostile intelligence services.

Another point to remember is that the operative of a foreign intelligence service need not be a foreigner, nor need the occasion of your encounter with him or her be in any way extraordinary. A routine acquaintance, for example, could in actuality be a diplomat from Eastern Europe or an American who has been recruited as an agent by a hostile intelligence service. He/she could be a "spotter," who reports to an intelligence service on people he/she meets who appear to be susceptible for recruitment, and then arranges for intelligence officers to meet them.

Do not expect either the intelligence officer or agent to expose his/her role in any dramatic or sudden fashion. Usually there is a long period of cultivation during which conversations appear completely innocuous. At any point where someone begins to inquire aggressively into aspects of your knowledge or activity, which are classified or otherwise sensitive, you should certainly stop to consider whether the inquiry is simply, innocent curiosity. It might be the beginning of an attempt to secure sensitive information for the benefit of another country.

If an employee has dealings with representatives from the Soviet Union, Bloc countries, Cuba, or the People's Republic of China, there are a number of defensive steps that can be taken. The most important step is to have all such contacts reported to your Security Officer. This allows the Security Officer to monitor the contacts and to protect the employee's record. It also enables the Security Officer to detect recruitment operations as they develop.

Secondly, efforts should be made to recognize when an association evolves from one of strictly business to one of a more personal nature. In recruitment scenarios, a key first step taken by intelligence officers is the development of a personal rapport and social relationship with targeted individuals. This must be recognized. Casual meetings away from the office should be avoided. Gifts or special favors should not be solicited or accepted. One further defensive technique is to avoid one-on-one meetings. Needless to say, the more people involved in a meeting, the less opportunity there is for an intelligence officer to develop a personal rapport or to ask the employee questions he/she does not want to answer.

In general, the role of the Security Officer must be stressed. Each Government agency and private firm which deal in classified material has, or should have, a designated official responsible for security matters. This Security Officer should be recognized as an ally and not an adversary. If you become involved in a situation that arouses your suspicions, the Security Officer should be informed immediately. Even if a friendship has been established, and the individual has been

able to pry loose some information, the Security Officer's job is to minimize the damage that the loss of sensitive information may cause, protect employees from getting ensnarled in situations involving hostile intelligence services, and to extricate them when necessary. This assistance cannot be rendered if the employee remains silent. Of course, it is much better for an employee to reveal a suspect relationship voluntarily, rather than have it come to light in the course of an investigation. In sum, if involved in a compromising situation, the sooner the employee consults his/her Security Officer, the better for all concerned, the employee, the employer, and the United States.

You may be in a place or situation where you cannot, or for some reason do not want to, contact your Security Officer. In the United States, the FBI is as close as your nearest telephone. Abroad, the nearest U.S. diplomatic establishment can arrange to put you in touch with the FBI or other appropriate U.S. Government security officials. Once again, it must be stressed that your best course of action in any of the situations described above is to relate the facts to a professional who will be able to analyze the situation and propose a course of action. Any attempts by untrained or uninformed persons to handle hostile intelligence efforts on their own could result not only in personal disaster, but may also interfere with the FBI's counterintelligence effort.

The threat posed by hostile intelligence services can easily be underestimated. History is replete with situations in which a nation's security was gravely damaged by the efforts of a hostile nation's intelligence services. The breaking of the Japanese diplomatic code helped to bring United States victory in the Pacific during World War II. On the other hand, the theft of some of our key atomic secrets greatly abetted the interests of the Soviet Union. The work of hostile intelligence services is by no means trivial; the fates of nations have been damaged or enhanced by their enterprises.

A philosopher once said, "Knowledge itself is power." This maxim applies to national power. One gauge of national power is the quantity and quality of scientific, technological, political, and military-related knowledge possessed by a nation. The United States can be weakened by the theft of its vital knowledge. Its enemies can be strengthened by the acquisition of that knowledge, whether classified or unclassified. It is the responsibility of each individual, who has been entrusted with sensitive data, to do his or her share in protecting America's strategic knowledge. If Americans do not conduct themselves in a responsible manner, or do not recognize that this country's national security is based upon the loyalty and efforts of its citizens, then the tightest document classification system, the most efficient security organizations, and the strongest armed forces may be completely ineffective in protecting its citizens from "all enemies, foreign and domestic."