

Counterintelligence

Table of Contents

Introduction	2
Human Intelligence Threat	3
What is Human Intelligence?.....	3
Who is Targeting the United States?	3
What Are They After?.....	4
Why Are We Vulnerable?	5
How Is Human Intelligence Conducted?	6
Spotting and Assessing Potential Targets	7
Operations in the United States	8
Operations Outside the U.S.....	10
Motivation and Recruitment	13
Life after Recruitment	14
Information Collection.....	14
Communications	15
How Are Spies Caught?	17
Observation of Espionage Indicators	17
The Spy's Own Mistakes	18
Insider Espionage Is a Growing Threat	19
Opportunity for Espionage	20
Motivation for Espionage	21
Interaction Among Trends	23
Implications	23
Reporting Espionage Indicators	24
Making the Right Decision	25
Making the Wrong Decision.....	27
Behavior Patterns and Personality Characteristics Associated with Espionage	28
Antisocial Behavior	30
Example: John Walker	31
Narcissism/Grandiosity.....	32
Grandiosity.....	32
Entitlement	32
Lack of Empathy	33
Example: Jonathan Pollard	34
Impulsiveness/Immaturity.....	35
Example: Robert Hanssen	36
Inability to Form a Commitment	37
Example: Christopher Boyce	38
Vindictiveness.....	39
Example: John Walker	39
Paranoia	39
Risk-Seeking	40

Example: Aldrich Ames	41
Example: John Walker	41
One Country's Program to Obtain U.S. S&T Secrets	42
In the Line of Fire: American Travelers Abroad	47
Potential CI Risk Indicators.....	51
Use of CI Risk Indicators For Personnel Security Decisions	53
Potential Indicators of Being Or Becoming a Target for Recruitment.....	54
Circumstances Beyond the Subject's Control	54
Behaviors that Attract Foreign Attention	56
Indicators of Already Being a Target	57
Potential Indicators of Susceptibility To Espionage or Terrorist Activity ...	58
Indicators of Conflicting Interests	58
Indicators of Vulnerability to Pressure or Duress	59
Indicators of Competing Identities	61
Indicators of Personal Weaknesses	62
Potential Indicators of Espionage, Terrorism, or Subversive Activity.....	64
Indicators of Recruitment	64
Indicators of Information Collection	65
Indicators of Information Transmittal	66
Indicators of Illegal Income	67
Indicators of Terrorist Activity	68
Indicators of Support for Terrorism.....	69
Other Behavioral Indicators	70

Introduction

Our cleared personnel are primary targets of foreign intelligence services. They are the keepers of the nation's secrets and are often working in exposed and vulnerable positions overseas or working with foreign nationals. The background investigation process is designed to provide assurance that personnel are reliable, trustworthy, loyal to the United States, and not vulnerable to foreign manipulation or coercion.

While procedures vary among agencies, the adjudicator of security clearances is in a unique position to look at the completed background investigation from a counterintelligence perspective and, in fact, may be the only person who is actually trained to do so. Knowledge of the threats posed by foreign intelligence services and the techniques they use to recruit and run spies is crucial to proper evaluation of potential indicators of counterintelligence risk that may be identified during the initial background investigation or periodic reinvestigation.

This module provides information that will allow personnel security investigators, adjudicators, and managers to recognize vulnerabilities that can be exploited by foreign intelligence collectors and understand how they do so. It provides a comprehensive list of counterintelligence risk indicators. It also discusses the vulnerabilities in espionage tradecraft that create opportunities for espionage to be detected by a knowledgeable observer.

The National Security Act of 1947 defines counterintelligence as “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.”¹ This definition has held up well over the past 60 years. While counterintelligence is concerned with all intelligence threats, including foreign collection of information from technical sources and open sources, this Counterintelligence module deals only with the insider threat -- the threat of espionage, terrorism, sabotage, or subversion by Americans with access to classified or other controlled or protected information.

Human Intelligence Threat

What is Human Intelligence?

Human intelligence, often called HUMINT, is simply the use of human beings as sources of intelligence information. It is the traditional spy, as well as the interrogation of detainees, and elicitation of information from unwitting persons. Despite the great advances that have been made in technical means of intelligence collection with satellites and communications intercepts, HUMINT remains uniquely valuable.

In the information age, human sources have access to vast quantities of information that can be carried out of a secure facility on devices smaller than a ball point pen. Transmittal of that information can be accomplished instantaneously, and it can be used to cause the death of our citizens and allies. Information about our weapons systems, technology, plans, and intelligence collection systems can negate the expenditure of many billions of dollars and seriously damage our ability to accomplish military missions, economic objectives, or foreign policy goals. To help counter this threat, personnel charged with security responsibilities need to understand that threat and their role in protecting against it.

Who is Targeting the United States?

America's role as the dominant political, economic, and military force in the world makes it the number one target for foreign espionage. As the largest economy in the world, the United States is seen as a competitor as well as a valuable market. We spend large sums on a broad range of research and development projects that are not available to the rest of the world. The results of that effort are very attractive to both foreign governments and foreign companies, because copying this research and development can save them millions of dollars and provide economic and military advantages. In addition to the intelligence services of friendly as well as unfriendly countries, sources of the threat to classified and other protected information include:

- Foreign or multinational corporations.
- Foreign government-sponsored educational and scientific institutions.
- Freelance agents (some of whom are unemployed former intelligence officers).
- Computer hackers.
- Terrorist organizations.
- Revolutionary groups.
- Extremist ethnic or religious organizations.
- Drug syndicates.
- Organized crime.

Individuals in both government and industry in almost 100 countries were involved in legal and illegal efforts to collect intelligence in the United States during 2004 .[2](#) In addition, literally dozens of terrorist and criminal organizations are also engaged in intelligence collection efforts directed at the United States. The bulk of the activity, however, originates in a relatively small number of key countries. The National Counterintelligence Executive estimates that the top 10 collectors probably account for 60 percent of the suspicious foreign collection efforts against U.S. cleared defense contractors.
[2](#)

The U.S. Government, as a matter of policy, does not identify publicly which foreign countries represent the greatest intelligence threat. To do so would create a false sense of security when dealing with any of the unnamed countries, and such a list would soon be out of date. The key countries include friends and allies as well as strategic competitors. They conduct espionage against the United States for one or more of the following reasons:

- The country competes with the United States for global or regional political and economic influence.
- The country feels threatened by a hostile neighbor and seeks to develop or obtain the most advanced military technology. It may also seek information on U.S. policy, and to influence U.S. policy, toward itself and the neighboring country.
- The country has a developing economy and sees its economic future as being dependent upon the rapid acquisition and development of new technologies by every possible means, whether legal or illegal.
- The country competes with U.S. companies in the global marketplace for the sale of advanced technologies or military weaponry.

What Are They After?

What are the spies and other intelligence collectors after? Everything that will help another country, organization, corporation, research institute, or

individual achieve its political, military, economic, or scientific goals. It is important to realize that the scope of foreign intelligence interest in the United States is virtually unlimited. The most critical areas include future military and political intentions, military capabilities and vulnerabilities, economic and commercial policies, and foreign policy initiatives. Increasingly, however, technology ranks high in foreign collection priorities.

Technology that is critical to the protection of national security, including U.S. military superiority and qualitative advantage, is subject to U.S. security and export controls. These technologies, plus proprietary information that can provide economic advantages, are principal targets of foreign intelligence collectors.

Areas of technological interest change rapidly and can be very broad, but those of military concern are periodically collected and published as the Militarily Critical Technologies List (MCTL). As of 2004, the technologies on the MCTL that were most sought after by foreign intelligence collectors included: information systems (software and hardware), sensors (the eyes and ears of many military systems, including high-speed cameras, night vision equipment, and sensor platforms placed on unmanned aerial vehicles), aeronautics (unmanned aerial vehicles, composite materials, onboard computer management systems, experimental aerospace platforms), and electronics (used in virtually every weapons system to enhance performance and reliability while reducing size and increasing power.) [2](#)

A current MCTL is available at <http://www.dtic.mil/mctl>. There is detailed information on each technology that is subject to export control and other regulations, as well as a general discussion of how this technology is used by the military.

Why Are We Vulnerable?

At the same time that the United States is increasingly a target of intelligence collection, we are in many ways becoming increasingly vulnerable to intelligence attack. This is discussed in greater detail in a separate file called [Insider Espionage Is a Growing Threat](#). The head of the National Counterintelligence Executive, Michelle Van Cleave, listed some of our vulnerabilities as follows in September 2005 testimony to Congress: [3](#)

- Our general culture of openness has provided foreign entities easy access to sophisticated technologies. Each year, for example, we allow tens of thousands of official foreign visitors into U.S. Government-related facilities such as military bases, test centers, and research laboratories. Some of these visitors are dedicated to acquiring U.S. technology and know-how not otherwise available.
- American colleges and universities are centers for high-tech development that employ large numbers of foreign-born faculty and

train large numbers of foreign students, many of whom will return to their home countries. For example, an increasing number and proportion (approaching 30 percent) of science and engineering faculty employed at U.S. universities and colleges is foreign-born, according to National Science Foundation statistics. Moreover, the most recent data available indicate that about 40 percent of Ph.D. degrees awarded by U.S. universities in technical sciences and engineering -- roughly 8,000 per year -- now go to foreign students. The vast majority of these students are legitimately studying and advancing academic pursuits. But some are not.

- Breathtaking advances in information technology have vastly simplified the illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data as well as classified information. Compact storage devices the size of a finger and cell phones with digital photography capability are some of the latest weapons in technology transfer.
- Sophisticated information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to cyber exploitation. Many nations have formal programs for gathering our network information, and foreign competitors are developing the capability to exploit those vulnerabilities.
- Globalization has mixed foreign and U.S. companies in ways that have made it difficult to protect the technologies these firms develop or acquire, particularly when that technology is required for operations overseas. In 2004 alone, according to the Department of Commerce, foreign investment in the United States amounted to more than \$100 billion.

In addition, the global war on terror has led to the deployment of many thousand U.S. military, government and contractor personnel to high-risk areas overseas. This war has also tested the loyalties of some U.S. citizens.

How Is Human Intelligence Conducted?

In theory, intelligence collection is a carefully planned enterprise that follows these steps:

- Identify the valuable information to be collected.
- Determine where this information is located.
- Determine who has access to the information.
- Contrive a means to meet and assess individuals with access to the desired information.
- Identify a susceptible individual and then recruit that person as an agent.

- Maintain some means of secure contact with the agent and receive a steady flow of valuable information.

As in most complex activities, however, there is often a gap between theory and actual practice. It is difficult for foreign intelligence collectors to identify Americans who are willing to spy for a foreign country. If a foreign intelligence officer is operating within the United States, he or she has to do it without getting caught, and this imposes many constraints on what they can do.

Although much intelligence collection against softer targets, such as defense industry and the scientific community, follows this theoretical model, intelligence collection against the harder targets is much more opportunistic. The intelligence collector grasps whatever opportunities become available. Indeed, most Americans who became spies during the Cold War volunteered their services to a communist country. They were not the product of a deliberate process of spotting, assessment, and recruitment. The current global environment is now much more conducive to the systematic assessment and recruitment of Americans by foreign intelligence services.

Spotting and Assessing Potential Targets

Once a collection requirement has been identified, the first step undertaken by a foreign intelligence service or agent is to determine where the desired information is located. This could be a specific government office, company, academic or scientific institution, or geographic location. The next step is to identify specific persons with access to the desired information and then to start collecting information on those persons.

This is commonly accomplished through open sources to the extent possible. The Internet provides an abundance of avenues for helping foreign intelligence collectors identify and assess intelligence targets. This includes searching the Internet for references to a target company in newspaper accounts, blogs, and Internet chat rooms, and identifying individuals who have published articles on a topic of interest. Information can often be elicited at conferences or meetings or during official visits to an installation. Acquisition of an organization's internal phone book is a common goal.

A foreign intelligence or security service will also identify people or organizations in its own country that have contact with the target organization. People who are familiar with target organizations or individuals will be interviewed. Visa or border control records will be checked to see if a target individual has traveled to his or her country. An organization or individuals within the organization may be put on a watch list for communications intercepts.

The next steps are assessment and recruitment. There are significant differences between how foreign intelligence services operate in the United

States, where they are at risk of being detected, and how they operate on their home turf where risk is low and they have all the national resources available for their use.

Operations in the United States

Countries with an active intelligence collection program in the United States generally have several different types of assets here. They have professional intelligence officers whose job is to spot, assess, recruit, and handle agents or to support such activities in various ways. These operate under cover in an effort to conceal their role as intelligence officers. This means their cover job ties up most of their time. Some are in their embassy, a consulate, or an international organization that provides diplomatic immunity in case they are caught. Some have cover positions in a trade mission, as a newspaper correspondent, or as a businessman. These do not have diplomatic immunity and are subject to arrest if caught.

Others are sent to this country as agents rather than as professional intelligence officers. Their task is to penetrate a specific organization, identify or cultivate targets for recruitment, collect a specific type of information, or arrange for the illegal export of controlled technology. To achieve these goals, they come here for various ostensibly legal purposes, such as to open a business, participate in exchange programs or joint research projects, to monitor contracts for the manufacture and purchase of U.S. military equipment, or as visiting scientists or doctoral students.

For example, if a foreign intelligence service is targeting a highly specialized topic, such as high energy physics, the service might identify one of its own nationals who is an expert in this field. This individual will then be given intelligence training and inserted into a position that provides access to the needed information, or access to the foreign nationals who have this information. The tasking might be limited to cultivating selected attendees at international conferences, or the agent may be dispatched to the United States on one of the many exchange programs.

The professional intelligence officer will operate by developing as wide a circle of contacts as possible through membership in organizations, attendance at conferences, symposia, etc., and by exploiting all the possibilities inherent in his or her cover position. Different cover positions offer access to different groups of people. Many intelligence officers under cover in an embassy or as journalists work the diplomatic cocktail circuit and Capitol Hill. Others under cover in a consulate or trade mission work the émigré community or the business community.

Finding some means to establish personal contact with a target, either directly or through an intermediary, may involve an imaginative cover story. Some of the known ploys are various versions of the unsolicited email request for assistance and the ostensible headhunter interview to assess the

target's interest in and qualifications for a job vacancy at another company. If the target is an emigrant from the intelligence officer's country, it may be possible to arrange a contact through émigré connections.

Once the initial contact is made, there is a process for assessing and developing targets for recruitment that is followed by most intelligence services. It is sometimes called the "road to recruitment." The first goal is to find or create some basis for further meetings. The intelligence officer then tries to become a friend, learning what makes a person tick, sympathizing with their problems, and feeding their ego. The rituals of espionage like secret meetings and dead drops are avoided, at least at the beginning. The goal is to make it easy for the target to become a friend. Developing some type of personal bond of common interests is much easier if the intelligence officer and the target share the same national, ethnic, or religious background.

If the target can be maneuvered into talking about things like the high cost of putting his two sons through college, the medical bills for his daughter's leukemia, disagreements with U.S. Government policy, or the unfairness of his boss, this is noted as a possible source of motivation for cooperation. If the target seems amenable, the intelligence officer will talk about topics of intelligence interest that are easy for the target to rationalize talking about, looking for ways to gain one small step of cooperation at a time. To gain sympathy, the intelligence officer may talk about his country's need for economic development or the threat from his country's enemies.

As this cultivation proceeds, the intelligence officer will try to create some basis for the target to feel obligated to the intelligence officer. The sense of obligation might be created by a prospective business deal, invitation to a foreign conference or seminar in the intelligence officer's country, information provided by the intelligence officer or access to influential people arranged by the intelligence officer, loans or grants, or assistance to relatives in the foreign country. If this is done right, the target may not know this is a spy operation until he or she is so far down the road to recruitment that he or she is either afraid to turn back or does not want to turn back.

Of particular interest from a personnel security perspective are those intelligence officers assigned to work their country's émigré community in the United States. These officers are often under cover in a consulate, rather than the embassy, where their overt functions include assisting emigrants in the United States who have problems with the home country or the U.S. Government, encouraging and facilitating travel to the home country, and promoting the culture of their home country. For example, intelligence officers under cover in the consulate are likely to handle the dealings with émigrés who contact the consulate to surrender their passport or renounce their citizenship.

Those intelligence officers who specialize in the émigré community have two goals: (1) to penetrate and monitor the activities of dissident groups who are opposed to the intelligence officer's current government, and (2) to spot, assess, and recruit émigrés who have access to information of value to the home country. For some developing countries, the legal or illegal acquisition of foreign technology to support the country's economic development and military strength is viewed as a national mission, not just an intelligence collection program.

Some countries with sizable émigré communities in the United States maintain detailed records with background information on their émigrés, their technical or scientific specialties, and where they are currently employed. These countries use such records to support open programs to recruit experienced engineers and scientists to return to their home country to contribute to the home country's economic development. These same programs are used to assess and recruit individuals to provide sought-after classified or other controlled information while remaining in the United States. One such program is discussed in detail in a separate file in this module entitled [One Country's Program to Obtain U.S. S&T Secrets.](#)

When a relationship is established that involves repeated meetings, this creates a security dilemma for the intelligence officer. He does not want the target to talk about the meetings or for the meetings to be observed and reported. However, if he asks the target to keep the meetings secret, the target may become frightened and withdraw from the relationship. When a relationship progresses to the point where the target agrees it is advisable to meet discreetly so they will not be observed, this marks a significant step forward on the road to recruitment.

Foreign intelligence operatives in the United States are careful to avoid being caught committing any offense for which they can be arrested or, if they have diplomatic immunity, be expelled from the United States. Even those with diplomatic immunity want to avoid being expelled, as that limits their future foreign assignments and is not career-enhancing. They also need to be careful to avoid traps laid by the FBI. To avoid or minimize the potential adverse consequences of an unsuccessful recruitment approach, arrangements are often made for the target to travel to the intelligence officer's home country for some reason, and the recruitment is done there.

Operations Outside the U.S.

When foreign intelligence services are operating at home, the operational environment and their capabilities are very different than in the United States. They can operate aggressively on their home turf because there is no risk of being caught. They have access to all the resources of the local government including police, customs and border control authorities, financial organizations, universities, and businesses. Therefore, they can monitor and, to some extent, control the environment in which an American

living in or visiting their country lives, plays, and works. Americans, by contrast, are at a disadvantage, because they are in unfamiliar territory.

In many cases, the foreign intelligence service will know in advance that a target of interest is coming to their country. The forthcoming trip will have been reported, and in some cases arranged, by one of their intelligence officers or agents in the United States.

Others are identified as targets only as a consequence of their trip to that country. American visitors draw the intelligence or security service's attention when they:

- Are attending an international meeting dealing with science or technology, trade, foreign policy, or any other topic of potential intelligence interest.
- Come for negotiations with the foreign government or a local corporation.
- Have family, friends, or business contacts in the country who can provide information about them.
- Behave in a manner that indicates possible susceptibility to recruitment. The local drug scene, prostitution, gay and pedophile hangouts, black market currency exchanges, gambling establishments, dissident groups, and illegal sale of antiquities in some countries are typically monitored by police informants who report the involvement of foreign nationals in these activities. These are areas where human weaknesses may be observable and exploitable. Informants in these areas may also be used to provoke a target into becoming involved in such activities.

Operations against Americans visiting or residing in the foreign country are of two types. One is to simply steal or elicit information of value without trying to recruit the American, while the other is the traditional effort to assess and recruit Americans as spies.

Exploitation Without Recruitment: In many countries, U.S. Government officials, scientists, engineers, and businesspersons who are known to have valuable information are targets even if there is no hope of recruiting them as agents. Information can be obtained from them in other ways. This includes Americans who come for discussions or negotiations with the government or other major organizations or corporations. The intelligence service seeks to obtain from them information to help its country gain the best possible outcome from these discussions. U.S. intelligence does not conduct intelligence operations for the benefit of U.S. corporations, but other countries with aggressive intelligence services do, especially for corporations that are controlled by their government.

The tools for obtaining information are surreptitious entry into laptop computers, briefcases, and suitcases left in the visitor's hotel room; secret monitoring or recording of phone conversations that take place in hotel rooms, offices, meeting areas, and sometimes restaurants; intercepting phone, fax, and e-mail communications when feasible; and sophisticated elicitation techniques. These kinds of operations are all commonplace in a number of countries, including some countries who are friends and allies of the United States. A separate file entitled, [In the Line of Fire: American Travelers Abroad](#), has twenty anecdotes reported by American scientists about their experiences during travel overseas on official business to attend meetings and conferences and to perform research.

In some countries, the security service has its own offices in the principal hotels used for large conferences. It takes only a minute or two for someone to enter a hotel room and bug the telephone so that all room conversations can be monitored from a line connected to the hotel switchboard.

Office communications are also vulnerable to monitoring. Many foreign telecommunications companies are owned or controlled by the government. Even those not government-owned or controlled are regulated by the government and will normally cooperate when their government requests assistance in monitoring specific lines. Under such controlled circumstances, it is easy to intercept any form of electronic communications. Legal restrictions governing technical surveillance that apply in the United States have not been adopted by most other countries with which we have close trading ties.

Elicitation of valuable information during a seemingly normal professional or social conversation is also surprisingly effective, as most of us want to be polite and helpful, appear well-informed about our professional specialty, and be appreciated for our work. We also don't want to be suspicious of other people's motives and are uncomfortable telling lies. Trained intelligence operatives take advantage of these good qualities to get us to tell them things about ourselves, our colleagues, or our work that ought to be kept to ourselves.

Assessment and Recruitment: The process for assessing and developing a target for recruitment differs somewhat from how it is done when operating in the United States, as far more resources are available to the intelligence officer. It may also be greatly accelerated if the target is visiting the country and accessible for only a short time. When operating in the home country, the approach is more likely to include efforts to entangle the target in sexual or other activities which are questionable morally or legally, and more likely to combine persuasion and incentives with pressure and coercion if that becomes necessary to achieve the goal.

Relatives, business contacts, sexual partners, tour guides, taxi drivers, and anyone else having contact with a potential target can be asked about the

target, and some will be recruited as informants. An intelligence officer can use a variety of ruses and covers such as a journalist, researcher, businessman, tourist board representative, public opinion pollster, or policeman to establish direct contact with the target in order to assess reactions to various questions or circumstances. Operationally useful information may be available from searching the target's hotel room, monitoring the target's phone conversations, or other technical sources.

Depending upon the results, the target may be dropped, the intelligence service may move forward with a recruitment approach, or arrangements may be made for continuing assessment. If the target is returning to the United States, some guise may be found to maintain contact to discuss a possible business proposition or research assistance or to discuss any other common interest, or a pretext may be found to introduce the target to another intelligence officer in the United States.

Motivation and Recruitment

Many years ago, the conventional wisdom was that the only Americans who would spy against their country were communists or persons coerced against their will. In more recent years, the conventional wisdom has been that most Americans who betray their country's secrets do it for money -- either financial need or greed. It is true that most spies are paid for their services, but motivation is often more complex than that. Most Americans are in need of money, or want more money for whatever reason, but very few are willing to commit espionage to get it. So need and greed are relevant factors, but these factors alone are not predictive of willingness to commit espionage.

Broadly defined, motivation is a state of mind that influences one's choices. Motivation for espionage generally results from a complex interaction between personal characteristics and the situation in which the person finds himself or herself. The separate file on [Behavior Patterns and Personality Characteristics Associated with Espionage](#) discusses some of the relevant personal characteristics.

The intelligence officer's goal when assessing a target is to figure out what is so important to that person that it can move him or her to action. Money is certainly one possible motivator, but it moves a person to action such as espionage only if other personal beliefs, character weaknesses, or emotional needs are present as well.

Weaknesses or vulnerabilities that a foreign intelligence officer will try to identify and exploit include the following:

- Feelings of loyalty or obligation to the intelligence officer's country based on common national, ethnic, or religious background, friends or relatives in that country, or disagreement with U.S. policy toward that country.

- Interest in the welfare of one or more relatives or friends in the intelligence officer's country. The officer might induce cooperation by arranging some type of benefit (housing, job, health, education) for a relative or friend. Positive inducement is more likely to be effective than threatening harm.
- Anger or bitterness toward employer.
- Willingness to violate commonly accepted social norms -- cheating, lying, stealing, selling drugs, etc. (Another way to look at this is that values which normally inhibit illegal or vindictive behavior are missing.)
- Attraction to adventure and taking risks.
- Needs for praise, to feel important, or for recognition of how clever one is.
- Any circumstance that creates an urgent need for money, such as children going to college, a serious illness of child or spouse, costs associated with divorce, lost income due to spouse's loss of job, large gambling losses, imminent retirement but with inadequate savings for a retired lifestyle, or imminent risk of bankruptcy.
- Vulnerability to pressure. Can the target be intimidated? Is the target afraid of the country's security service?

How the foreign intelligence service structures the recruitment approach varies greatly depending upon the assessment of what might motivate the target to agree. One common practice is to proceed gradually, starting with requests for small favors that seem innocuous and building up gradually to more sensitive tasks. This recognizes that it takes time for many people to adjust to the fact that they are becoming a spy and to reconcile this with their own self-image. If the target balks at some point, the intelligence officer can point out that he or she has already been cooperating with an intelligence service for a long time and has been paid for this service, so there is no turning back now.

Life after Recruitment

Once a new agent is formally recruited, the asset is trained first in security, then in a plan for maintaining communications, and finally in what information to collect and how to collect it.

Information Collection

The targeted information may come from access the agent has by virtue of his or her position, from the agent's association with other people with access to sensitive information, or occasionally just by virtue of the agent's ability to enter a certain area and observe. Some agents provide support to other agents or report on other persons who might be recruitable. Still others

might be recruited to use their influence in ways beneficial to the country sponsoring the espionage.

The most valuable agents are usually those with direct access to information sought by the foreign intelligence service. If they do not initially have such access, many foreign services will devote considerable time and effort to working them into positions where they do have direct access. Many low-paying, low-prestige jobs such as mail clerks, maintenance personnel, and janitors are attractive to an intelligence service. They have physical access to protected documents or sensitive meeting rooms, and these jobs have high personnel turnover which makes it easier to plant an already-recruited agent in such jobs.

Once in a position with access, the agent collects information either by observation or by taking documents or electronic media out of the facility where the agent works. Physical security controls when exiting buildings have proven to be only a limited deterrent to removing information from secure facilities. If necessary, most intelligence services can provide their agents with technical equipment such as photo and recording devices or concealment devices. Modern information technology allows the transfer of huge amounts of data to very small devices.

Intelligence services prefer to receive copies of original documents rather than an agent's oral or written report on a conversation or personal evaluation of events, because documents are far more authoritative. An agent may be under considerable pressure to collect large amounts of material, often in areas he or she would not normally have a need to see or use, and payment will often depend upon the value of the information provided.

Collecting and copying protected information and removing it from a secure facility can be a source of danger for the agent in an office where effective document controls and computer audits are in place. Pressure to meet the foreign intelligence officer's requirements for more documentary data on specific subjects or a desire to earn more money can cause an agent to take greater risks that can sometimes lead to the agent's detection. There are a number of observable indicators of such information collection that coworkers are supposed to report to their supervisor or to security when they are observed. These indicators are discussed in a separate file, [Potential CI Risk Indicators](#).

Communications

The method of communications that is selected depends upon the amount and format of material to be communicated, the urgency or timeliness of the information, the ability of the agent to travel to meetings outside the United States, how much handholding is required to guide the agent's collection of information or maintain the agent's motivation, and the technical capabilities

of both the intelligence service and the agent. There is a host of possibilities, all of which entail a different level or type of risk. Communication is of two types: personal communications, where there is face-to-face contact, and impersonal communication where there is no personal contact.

Personal Communications: Personal communications can vary from a several-day training session to a "brush pass" where a packet is passed surreptitiously between the agent and the intelligence officer as they cross paths. Personal meetings are the most risky as the intelligence officer or the agent may have been identified by a security service and be under surveillance. Though risky, personal meetings are sometimes necessary for training or to keep the agent motivated.

Personal meetings are particularly useful for training and for monitoring an agent's motivation, which may change over time. Personal problems that led the agent to become involved in espionage may improve or get worse. Motivation may be affected by the stress of leading a double life or by changes in world affairs. The intelligence officer needs to be sensitive to such changes.

Foreign intelligence services have favored overseas locations for personal meetings since there is less risk to the intelligence officer. This is particularly true for longer meetings when a new agent is trained. The time between meetings varies as needed. Meetings with a new agent may be held monthly while several years may pass without a need to meet an established agent. Some intelligence services have supplied their agents with false passports for operational travel so that no pattern of travel is apparent to security services. Agents with dual citizenship will sometimes travel for operational purposes on their foreign passports. Weekend and holiday travel is often favored so that the agent does not have to request time off from work.

Impersonal Communications: Impersonal communications do not involve any direct contact between the agent and the intelligence officer. The dead drop is the traditional means of impersonal communications. One or more locations are selected where either the agent or the intelligence officer can securely hide material without being observed. A schedule may be established for loading or unloading dead drops together with signals for communicating when a drop has been loaded and when it has been successfully unloaded. A signal may consist of a chalk mark on a building, telephone pole, or street sign that the agent passes daily on the way to and from work. For additional security, the dead drop may include use of a concealment device such as a fake rock or an old can.

Use of letters from the agent to the intelligence officer and radio transmissions from the intelligence officer to the agent have been common in the past. The letters are addressed to what is referred to as an accommodation address which is not openly associated with a foreign intelligence service, and the agent does not use his or her real return

address. The letters can contain information written in invisible ink, a concealed microdot photo, or open text messages where a seemingly innocuous phrase will have a previously agreed meaning. The radio transmissions are coded messages with instructions sent on the short wave bands.

Today, electronic communications are common. Information is only of value if it can be communicated to the users in a timely manner, and electronic media are the only practical means of communicating the large quantity of material that can now be downloaded from or copied off of large, automated information systems. Messages will usually be encrypted prior to transmission. Information may be communicated via the Internet almost instantaneously to virtually anywhere on the globe.

How Are Spies Caught?

Most Americans arrested and convicted of espionage or attempted espionage since the beginning of the Cold War were caught as a result of information provided by defectors from the foreign intelligence service or by American agents within the foreign intelligence service. The arrest of many others was the result of routine FBI surveillance of foreign embassies, surveillance of known foreign intelligence officers, and other standard counterintelligence practices. About 27% of those who succeeded in passing classified information to a foreign intelligence service were caught in less than one year. However, many of the most damaging spies betrayed their country for 10 or 15 years or more before being caught. [4](#)

Some American spies have also been caught as a result of observations of suspicious or unusual activity reported to a supervisor or to appropriate authorities by a coworker, friend, or former spouse. Many others went undetected for long periods because observations were *not* reported, or inadequate action was taken after they were reported.

Observation of Espionage Indicators

Being a spy requires that one engage in certain observable behaviors. There is usually some personal contact with a foreign intelligence operative who recruits the spy or to whom the spy volunteers his or her services. The spy must obtain information, often information to which the spy does not have normal or regular access. This information usually needs to be copied and then removed from the office. The information is then communicated to the foreign intelligence service, and this often requires keeping or preparing materials at home and traveling to signal sites or secret meetings at unusual times and places. The spy may receive large sums of money which then may be deposited, spent, or hidden. Periods of high stress sometimes affect the spy's behavior.

These behaviors associated with espionage or terrorism sometimes deviate from the norm in such a way that they come to the attention of other people who become suspicious and pass their suspicions on to others. This information occasionally comes out during a security clearance reinvestigation. A separate file on [Reporting Espionage Indicators](#) provides brief summaries of cases in which spies were caught because someone observed and reported suspicious activity, or were not caught because someone failed to report such activity. Another file on [Potential CI Risk Indicators](#) has a comprehensive list of espionage indicators.

Probably the single most observable change in a spy's behavior relates to money and how it is spent. Even spies who are not particularly well paid will usually find themselves with some disposable income. In this modern age, money almost always leaves a trail. This trail can be seen and followed, whether it is in the form of paid off debts or purchase of a new house, car, or boat. Neighbors notice, friends notice and, above all spouses notice. The new spy is forced to come up with explanations which usually will not stand close scrutiny. This is discussed further in the separate module on [Finances - Affluence](#). In the course of a background investigation, subject's explanation for his or her affluence should always be confirmed by documentary evidence provided to either the investigator or the adjudicator.

The Spy's Own Mistakes

Spying is a lonely business. To explain the changes in behavior, or because of a need to confide in someone else, spies sometimes tell a spouse or try to enlist the help of a friend. The friend or spouse in whom the spy confides often does not remain a friend or loyal spouse after he or she realizes what is going on.

Many people who betray their country are not thinking clearly, or they would not be involved in such a self-destructive activity. They are driven by emotional needs to feel important, successful, or powerful, to prove how smart they are, or to take risks or to get revenge. Some, in desperation, have sought through espionage to find a solution to severe financial problems. The same emotional needs that lead them to betray also cause them to flaunt their sudden affluence or to brag about their involvement in some mysterious activity. There is not much ego gratification if no one knows how affluent or important they have become, how they have gotten revenge on the employer who wronged them, or how they have cleverly outsmarted the system and gotten away with it.

When spies are driven by these out-of-control ego needs, they sometimes make mistakes that lead to their getting caught. The most common example of this is unexplained affluence. It is often asked why spies endanger their security by conspicuous expenditures beyond what they could afford with their salary. It is because, in many cases, hiding the money would defeat the purpose for which they committed the crime. In most crimes motivated by

greed rather than financial need, the money is sought because of its symbolic value. Money is a means to achieve or to measure social prestige, power or control, or to buy affection or gain self-esteem. The same compelling emotional needs that drive an individual to commit a crime like espionage often drive that person to spend the illegal income rather than save it or hide it.

Footnotes

1. 50 U.S.C. 401, National Security Act of 1947, enacted July 26, 1947.
2. Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage - 2005*. NCIX 2005-10006, April 2005.
3. Statement for the Record, National Counterintelligence Executive, The Honorable Michelle Van Cleave before the House Judiciary Subcommittee on Immigration, Border Security and Claims, September 15, 2005, page 2.
4. Herbig, K.L., & Wiskoff, M.F. (2002). *Espionage against the United States by American citizens 1947 – 2001* (Tech. Rep. 02-5). Monterey, CA: Defense Personnel Security Research Center.

Insider Espionage Is a Growing Threat

Because espionage is a secret activity, we cannot know how many undiscovered spies are currently active in American organizations or what the future will bring in terms of discovered espionage cases. Nevertheless, data are available to conclude that the prevalence of insider espionage may be significantly greater today than in the past, and may become more prevalent in the years ahead.

Opportunity and motivation are necessary and sufficient conditions for the crime of espionage. A study by the Defense Personnel Security Research Center (PERSEREC) examined technological, social, and economic trends that are affecting opportunity and motivation for insider espionage. It is assumed that if opportunity and motivation for insider espionage are increasing, then the frequency of espionage is probably also increasing. Conversely, if opportunity and motivation for insider espionage are decreasing, one might conclude that the frequency of espionage is also decreasing. [1](#)

The PERSEREC study identified and examined five trends that are resulting in increased opportunity for insiders to steal classified or other protected information and disseminate it to foreign entities. The term "other protected

information" includes dual-use or export-controlled technologies, trade secrets, and proprietary information. The study also identified and examined five trends that are increasing insider motivation to commit espionage. It is noteworthy that this research could not identify a single countervailing trend that will reduce either opportunity or motivation for espionage.

Opportunity for Espionage

Opportunity for espionage consists of access to classified or other protected information that can be exchanged for money or other benefits, means for making contact with minimal risk to foreign entities interested in obtaining this information, and means for transferring this information to foreign recipients. Technological, social, and economic trends that are increasing opportunities for insider espionage include: technological advancements in information storage and retrieval, an expanding market for protected U.S. information, the increasing globalization of commerce and scientific research, the increasing frequency of international travel, and global Internet expansion.

Information Technology: The development of large, networked databases with automated search functions increases exponentially the amount and variety of information a single malicious insider can access. Search functions make it possible to locate the specific data of greatest value to multiple foreign buyers. Rapid advances in the miniaturization of storage devices make it easier for insiders to remove without detection large quantities of information from the organization where they work. A memory stick or flash drive, also known as a "key chain drive" because it is small enough to carry on a key chain, or a "thumb drive" because it is only the size of a thumb, is readily available and can download up to 2 megabytes of data.

Expanding Market for Protected U.S. Information: Because of the increasingly competitive global economy and the increasing role of technology in the economic development of many countries, more allied and friendly countries are seeking to obtain protected U.S. technology by illegal as well as legal means. Some individuals who consider it reprehensible to sell American technology or military secrets to an avowed enemy of the United States may be less reticent to sell this information to individuals or organizations located in countries that are viewed as friendly to U.S. interests.

Globalization of Commerce and Scientific Research: The increasing globalization of commerce and research is greatly increasing the frequency of personal contact between knowledgeable insiders and foreign nationals potentially interested in exploiting their knowledge. This makes it easier for Americans to find foreign buyers for valuable information as well as for foreign intelligence operatives to locate willing American sellers of information. The frequency and nature of commercial and scientific relationships between American and foreign nationals also makes it more

difficult for personnel security and counterintelligence personnel to distinguish relationships that present a significant security risk from the many normal and innocent relationships that do not.

Increasing Frequency of International Travel: The continuing increase in foreign travel both to and from the United States means increasing opportunity for the transfer of classified and other protected information to foreign entities. Whether this interaction occurs in the United States or abroad, American insiders with access to valuable information are better able to establish contact with foreign buyers. Similarly, foreign nationals have more opportunity to spot, assess, and recruit American personnel. Again, because of the increasing number of contacts, it is becoming more difficult for personnel security and counterintelligence personnel to distinguish foreign travel and contacts that are of security concern from those that are not.

Global Internet Expansion: Just as the Internet creates a large and efficient marketplace for exchanging a wide variety of products and services, it can also bring potential buyers and sellers together for the illegal sale of classified or other protected information. It allows potential buyers and sellers of information to learn a great deal about one another, provides means for establishing contact (sometimes anonymously), and can be an efficient and relatively secure mechanism for transmitting almost unlimited quantities of information across national boundaries.

Motivation for Espionage

Motivation, broadly defined, is a feeling or state of mind that influences one's choices and actions. It is the result of a complex interaction between personality characteristics and situational factors. Most insiders with access to classified or other protected information possess personal qualities that are not conducive to committing espionage under any circumstances. However, some insiders will become motivated to commit espionage if they encounter the right conditions in their personal or professional lives. Situations that can result in motivation for spying include financial crisis, a gambling addiction, perceived mistreatment by one's employer, and feelings of obligation or loyalty to a foreign country or to a global community.

Increasing Prevalence of Personal Financial Problems: Of the many factors known to provide motivation for insider espionage, personal financial stress is among the more prominent. Serious financial pressure may cause an individual to turn to theft, fraud, embezzlement, or other illegal behaviors—including espionage—in an effort to alleviate financial pressures. Credit card debt as a percentage of income has been increasing for many years. Lending at high interest rates to individuals with poor credit histories, or who are already burdened with debt, has become a major source of profits and is one of the most rapidly growing segments of the consumer lending industry. The number of nonbusiness bankruptcies increased almost fivefold from 1985 to 2003. The 2005 bankruptcy law revision will significantly

increase the financial pressures on employees needing to file for bankruptcy due to unavoidable medical expenses, the loss of a job by a spouse, or divorce, as well as those whose problems are caused by irresponsible spending. Corporations are increasingly replacing the traditional defined-benefit retirement plan with 401(k) plans that shift the burden of retirement saving and investing to the employee. Many employees nearing retirement age lack savings to ensure a comfortable retirement.

Increasing Prevalence of Compulsive Gambling: Moderate gambling, like moderate alcohol use, is an accepted part of our culture. As with alcohol use, however, gambling to excess is a common weakness that can lead to serious security problems. As access to funds becomes limited, compulsive gamblers become more desperate and often resort to crime to garner the money required to pay their debts and sustain their addiction. Compulsive gambling is reportedly the fastest growing addiction among both adults and youth. The increasing prevalence of compulsive gambling suggests that an increasing number of insiders with access to classified or other protected information may become motivated to sell this information for money to pay off gambling debts.

Diminishing Organizational Loyalty: A lack of loyalty to one's employer, or resentment of an employer that results from perceived or real mistreatment, makes it easier for an insider to rationalize the theft and sale of the employer's information. Changing conditions in the American workplace suggest that the number of disgruntled employees may be increasing. In striving to compete in the global marketplace, American organizations increasingly engage in practices that alienate some employees. They more often downsize, automate, transfer jobs overseas, and lay off personnel who are no longer needed. They increasingly hire part-time and temporary workers who are offered limited benefits and minimal job security. Terminated American workers are less likely to receive severance pay, extended health benefits, or other types of assistance than in previous decades, and more often suffer from "layoff survivor syndrome" in which mistrust and anxiety has replaced feelings of fidelity to organizations. Many insiders with access to highly marketable technological information are transient workers who voluntarily move from one new employment opportunity to the next, cashing out their career investments on a regular basis.

Ethnic Diversification of the American Workforce: The United States has experienced a profound demographic transformation in the last three decades, resulting in a substantial increase in the number of American citizens with relatives, friends, or business contacts in foreign countries. The total foreign-born population in the United States almost tripled between 1970 and 2000. In 2000, over 10% of the U.S. population was foreign-born, and about 20% had one or more foreign-born parents. Emotional ties to family or friends in a foreign country, or to a foreign government, can result in conflicts of conscience concerning national loyalty. While many foreigners

continue to seek residence in the United States, more are coming to the U.S. for economic advantages rather than for political or ideological reasons. An increasing percentage of immigrants chooses not to become American citizens, and more of those who do obtain U.S. citizenship also maintain citizenship elsewhere.

Growing Allegiance to a Global Community: The increasing interaction between Americans and individuals of other nationalities appears to be resulting in a deeper global consciousness among many U.S. citizens and a greater appreciation of other cultures, religious beliefs, and value systems. Studies show that growing numbers of Americans—especially younger generations of Americans—are bicultural in that some aspects of their identity are rooted in local American traditions while other elements are rooted in an awareness of, and sense of belonging to, a larger global culture. These Americans feel a sense of loyalty to both the United States and other nations, simultaneously. They may include within their global community the people of countries that are currently conducting espionage against the United States. The increasing acceptance of global as well as national values may make it easier for a potential spy to rationalize actions that are actually driven by baser motives.

Interaction Among Trends

It is important to recognize that the vulnerabilities created by the technological, social, and economic trends presented here compound one another to create an insider espionage risk that is greater than the sum of its parts. That is to say, the risk presented by each trend is exacerbated by the risk that results from each of the other trends.

While it is significant that an increasing number of insiders have access to large networked databases, it is even more significant when they have this access AND can sell more different types of information to a broader range of foreign buyers...AND have greater opportunity to establish contact with and transfer information to foreign entities...AND are more vulnerable to experiencing financial crisis...AND are more vulnerable to becoming disgruntled and are less likely to feel an obligation to the organizations that employ them...AND have close personal ties to other countries...AND have a holistic view of the world that under some circumstances may result in their conceptualizing espionage as morally justifiable.

Implications

The obvious implication of these observations is that the incidence of espionage by insiders is likely to be greater today than ever before – and is likely to become more frequent rather than less frequent in the future. Since the technological, social, and economic trends discussed here are not amenable to government control, options for mitigating this increased vulnerability seem to be limited to: (1) reducing the frequency of insider

espionage by improving prevention, deterrence, and detection, and (2) reducing the damage that can be done by any single malicious insider by stricter monitoring of access to sensitive networks, compartmentation, and enforcement of need-to-know.

The security clearance process mitigates the risk of insider betrayal in three ways:

- To the extent that the investigation has a reputation for effectiveness, the process deters people with a history of unreliable, untrustworthy, or disloyal behavior from applying for a clearance.
- The initial investigation and periodic reinvestigation screen out individuals with alcohol or drug problems, serious criminal records, records of financial irresponsibility, serious mental health problems, and those who are vulnerable to foreign influence or who may have conflicting loyalties. These criteria are associated with unreliable, untrustworthy, or disloyal behaviors that run the gamut from simple failure to follow rules and procedures for the protection of information to the sale of information to foreign interests. To the extent that the personnel security screening is effective in achieving its goals, fewer unprincipled, irresponsible, troubled, or disloyal personnel who might be tempted or induced to become spies will gain or retain access to classified information.
- Careful investigation and review by well-trained personnel can identify indicators of possible betrayal of trust that are then referred for counterintelligence investigation.

Footnote

1. Kramer, L.A., Heuer, R.J., & Crawford, K.S. (2005). *Technological, social, and economic trends that are increasing U.S. vulnerability to insider espionage*. (Technical Report 05-10). Monterey, CA: Defense Personnel Security Research Center.

Reporting Espionage Indicators

Observant supervisors and coworkers are our first line of defense against insider threats, but often fail to recognize or report behaviors of significant security concern. Recent research that explored the underreporting of security-relevant behavior in the workplace shows that individuals are more likely to report when they understand that there is a direct link between the behavior their colleague is engaging in and national security interests. This indicates a need to educate personnel about a clearly defined set of indicators that an individual may be engaging in espionage or other

egregious behavior that must be reported¹ Questions asked during personnel security investigative interviews can help with this educational function and remind personnel of their reporting responsibilities.

This file provides brief summaries of cases in which American spies were caught because someone recognized and reported suspicious activity. It also provides brief summaries of cases in which espionage was allowed to continue undetected because coworkers failed to report suspicious activity or a supervisor failed to take the appropriate action when it was reported. All information about these cases is from public records except as otherwise noted.

A separate file in this Counterintelligence module, [Potential CI Risk Indicators](#), includes a comprehensive list of potential indicators of espionage or terrorism.

Making the Right Decision

The following stories are about people who made a difference by helping to catch a spy. When they saw or heard something that raised a suspicion, they chose to act. They made a call that helped to protect our national security.

Abuse of Authority

FBI intelligence analyst Leandro Aragoncillo used his access to FBI databases to search for and copy classified intelligence reports on the Philippines even though he had no need to have this information. When he found reports on the political climate and chances of a coup, he sent these by e-mail to opposition leaders in the Philippines. Aragoncillo is a naturalized U.S. citizen born in the Philippines. He spent 21 years in the U.S. Marine Corps, yet still felt so strongly attached to his native country that he wanted to help overthrow the current Philippine government.

After his arrest in September 2005, it was determined that Aragoncillo started accessing classified intelligence information and sending it to dissident political leaders in the Philippines in 2000, while working as a Marine staff assistant in the Vice President's office in the White House. Aragoncillo traveled back to his native country 15 times between 2000 and 2005, ostensibly at his own expense, despite having financial problems.

Aragoncillo was caught because he abused his authority as an FBI employee by intervening with the Immigration and Customs Enforcement (ICE) agency on behalf of a former senior Philippines police official who was arrested in New York on an expired visa. ICE advised the FBI, which prompted an FBI investigation leading to Aragoncillo's detection. His frequent travel to the Philippines and extensive downloading and copying of classified reports unrelated to his work could have been noted and prompted investigation earlier.

Unexplained Income

Dr. Ronald Hoffman managed a secret Air Force contract for Science Applications International Corporation (SAIC). From 1986 to 1990, he sold restricted space technology to four Japanese companies -- Mitsubishi, Nissan, Toshiba, and IHI Inc. -- and was paid over \$500,000. Hoffman was caught, prosecuted and convicted because an alert secretary saw something that didn't seem right, and reported it. She accidentally saw a fax from Mitsubishi to Hoffman advising of the deposit of \$90,000 to his account and requesting his confirmation that the funds were received. The secretary's husband was also suspicious of Hoffman's lifestyle -- two Corvettes, an Audi, a gorgeous sailboat and fine home that didn't seem compatible with his SAIC income.

Here's the secretary's message to others: "No matter what your level in the company, whether you are an engineer or just a clerk or even a person in the mailroom, don't be afraid to stick your neck out and say something. Be accountable."

Removing Classified Information from the Office

Jonathan Jay Pollard was a Naval Intelligence analyst arrested for espionage on behalf of Israel. He used his access to classified libraries and computer systems to collect a huge amount of information, especially on Soviet weapons systems and the military capabilities of Arab countries. Over a period of 18 months until he was arrested in November 1986, he passed over 1,000 highly classified documents, many of them quite thick. He was sentenced to life in prison.

The investigation leading to Pollard's arrest was triggered by a coworker who reported seeing Pollard take a package of Top Secret material out of the building about 4:15 p.m. on a Friday afternoon. Although the package was appropriately wrapped and Pollard had a courier pass to carry such material to a neighboring building, which was not unusual, it did seem suspicious at that time on a Friday, especially since Pollard got into a car with his wife. Investigation rapidly confirmed that Pollard was regularly removing large quantities of highly classified documents.

Reported Compromise of State Department Communication

Steven Lalas, an American of Greek descent, was a State Department communications officer stationed with the U.S. Embassy in Athens, Greece. He was arrested in 1993 and sentenced to 14 years in prison for passing sensitive military information to Greek officials. He began spying for the Greek government in 1977 while with the U.S. Army.

A report by a State Department official triggered the investigation leading to Lalas' arrest. This official reported the apparent compromise of a State Department communication. In a conversation with an official of the Greek

Embassy in Washington, the Greek official revealed knowledge of information that could only have come from a Secret communication between the State Department and the U.S. Embassy in Athens. Investigation pointed to Lalas, and this was confirmed by a videotape of him stealing documents intended for destruction.

Excessive Use of Photocopier

A coworker reported in 1986 that Michael H. Allen was spending excessive time at the photocopier in their office. This report led to investigation by the Naval Investigative Service. A hidden camera was installed near the photocopier in Allen's office. The resulting videotape showed Allen copying documents and hiding them in his pocket.

Allen was a retired Navy Senior Chief Radioman working at the Cubi Point Naval Air Station in the Philippines. He confessed to passing classified information to Philippine Intelligence in an effort to promote his local business interests. He was found guilty of ten counts of espionage.

Making the Wrong Decision

Many other spies remained undetected for a long period because observed indicators of espionage were not reported or, if reported, were not appropriately followed up. Our country suffered as a result.

Violations in Handling Classified Material

Navy spy Jerry Whitworth's work colleagues observed him monitoring and copying a sensitive communications line without authorization, saw classified papers in his personal locker, and knew Whitworth took classified materials home with him, but they believed he was doing it only to keep his work current.

None of these Navy personnel reported these improper activities before Whitworth's arrest in 1985 as part of the infamous John Walker spy ring. Their failure allowed the Walker ring to continue, with massive damage to U.S. national security.

Bragging About Selling Secrets

James R. Wilmoth was a U.S. Navy airman assigned to the carrier USS Midway in Japan. He was recruited by a Soviet KGB officer he met in a Japanese bar. As a food service worker he had no access to classified information. In order to be able to earn money as a Soviet spy, he recruited a friend, Russell Paul Brown, who took classified documents from the burn bag in the electronic warfare center of the Midway.

Although Wilmoth bragged about selling secrets to the Soviets, his comments were not taken seriously, so no one reported him. When his Japanese girlfriend sent postcards to Wilmoth's shipmates from vacation in Moscow, no one reported this either.

Excessive Use of Photocopier, Unexplained Affluence

Army Warrant Officer James W. Hall, III was sentenced to 40 years in prison for spying for both the former East Germany and Soviet Union from 1982 to 1988. He compromised U.S. and NATO plans for the defense of Western Europe. After his arrest, Hall said there were many indicators visible to those around him that he was involved in questionable activity.

Hall sometimes spent up to two hours of his workday reproducing classified documents to provide to the Soviets and East Germans. Concerned that he was not putting in his regular duty time, he consistently worked late to complete his regular assignments. Using his illegal income, Hall paid cash for a brand new Volvo and a new truck. He also made a large down payment on a home and took flying lessons. He is said to have given his military colleagues at least six conflicting stories to explain his lavish life style.

At one point coworkers observed a thick roll of \$100 dollar bills fall out of Hall's gym bag. They reported this to their Security Officer. The Security Officer failed to report the incident to counterintelligence. Instead, he called Hall in and asked about the money. Hall told him he had won the lottery, and the Security Officer was satisfied with that explanation. Hall continued to provide large amounts of very damaging information to the Soviet KGB and collected about \$100,000 for his services.²

Footnotes

1. Two relevant PERSEREC reports are available. Wood, S. & Marshall-Mies, J. (2003) *Improving supervisor and coworker reporting on information of security concern* and Wood, S., Crawford, K.S., & Lang E.L. (2005) *Reporting of counterintelligence and security indicators by supervisors and coworkers*. The latter is a succinct list of behaviors that clearly indicate an individual may be engaging in insider espionage, and which coworkers and supervisors should be required to report. For an electronic copy of either report send an email to perserec@osd.pentagon.mil.

2. The information about the roll of \$100 dollar bills and how this was handled is not available in the public record on the Hall case. It is from a personal communication to PERSEREC from Dan Christman, a retired Army counterintelligence specialist who worked on the Hall investigation.

Behavior Patterns and Personality Characteristics Associated with Espionage

There is no single profile of the employee who is likely to betray an employer's trust. However, clinical assessment of Americans arrested for espionage [1](#) and academic research findings on white-collar criminals in general [2](#) do identify a number of behavior patterns and personality characteristics that are commonly found among such persons. The following are discussed in this section.

[Antisocial Behavior](#)

[Narcissism/Grandiosity](#)

[Impulsiveness/Immaturity](#)

[Inability to Form a Commitment](#)

[Vindictiveness](#)

[Paranoia](#)

[Risk-Seeking](#)

Individuals who betray their employer's trust may have a propensity for violating rules and regulations. They may have a grossly inflated view of their own abilities, so that disappointment and bitterness against those who fail to recognize their special talents are inevitable. They may be inclined to regard criticism or disagreement as a personal insult that calls for revenge. They may be impulsive or immature, and predisposed to do whatever feels good at the moment. They may have drifted from one relationship or job to another, with little sense of purpose or loyalty to anyone or anything. They may engage in high-risk activities without thinking about the consequences.

Sometimes these weaknesses are so severe that they can be clinically diagnosed as symptoms of a mental, emotional, or personality disorder. More often, however, they are better described as behavioral or personality weaknesses rather than as psychological "disorders." When these behaviors are reported, consultation with a psychologist may be appropriate.

Because these weaknesses are also found to some degree in many good and loyal personnel, they are not specified in the Adjudicative Guidelines as disqualifying for access to classified information. However, they can and should be reported by investigators and used in the adjudicative process in the following ways.

- As a basis for adverse action if the behavior meets the disqualifying criteria under the Psychological Conditions or Personal Conduct guidelines.
- As part of a negative whole-person judgment. Financial problems, substance abuse and other issues are more significant when accompanied by some of the unfavorable behavioral or personality characteristics described here.
- As a basis for requesting further investigation, psychological evaluation, or psychological testing.

Antisocial Behavior

Behavior that habitually violates the commonly accepted rules of society is called antisocial behavior. Psychologists sometimes call a person who exhibits such behavior a psychopath or sociopath. Manipulation of others and deceit are central features of this type of behavior. John Walker, the infamous Soviet spy in the U.S. Navy who is described below, epitomizes antisocial behavior.

Antisocial behavior is a serious security concern. Values that normally inhibit illegal or vindictive behavior are missing. This can lead to fraud, embezzlement, computer sabotage or espionage when an individual sees an easy opportunity for illicit gain or becomes disaffected with the organization. Selling secrets may be viewed as a simple business opportunity rather than as treason

Persons with antisocial personality disorder shamelessly take others for granted and manipulate them to serve their own self-interest or indulge their own desires. Such persons take pleasure in beating the system without getting caught. Lying to others is common, as is lack of gratitude. Stealing, shoplifting, cheating on taxes, failure to pay parking tickets, aggressive or reckless driving, failure to pay bills even though money is available, picking fights, extreme promiscuity, sexual harassment, cruelty to animals, and spouse, child, or elder abuse are examples of antisocial behaviors. There is little remorse about the adverse effects of one's behavior on others.

At work, typical antisocial behaviors include padding travel vouchers or expense accounts; being consistently late to work or leaving earlier than is reasonable; abusing sick leave; lack of concern with meeting deadlines; taking classified information home; misusing the diplomatic pouch; pilfering office supplies; lying to cover up a mistake or to make oneself look good; maneuvering to undermine a colleague who is viewed as a competitor for promotion; drug use or any other violation of regulations by a government employee.

Antisocial persons tend to resent authority and dislike supervision, to attribute their lack of success to others "having it in for me," to think no one understands them and that life is giving them a raw deal. When antisocial individuals have a problem at work, they are likely to focus the blame on their supervisor. They may submit extensive written appeals in response to any criticism in their performance evaluation. When antisocial subjects feel offended or frustrated in their desires, they may be inclined to hold a grudge and to seek revenge.

Antisocial persons believe such improper behavior is commonplace and will not be punished. They have a high opinion of their ability to con their way out of trouble, and a low opinion of the astuteness of authorities who would catch them. The con man's self-confidence and ability to manipulate others

may be very useful in certain occupations (intelligence operations officer, undercover police officer, sales person), so it is sometimes difficult to distinguish a valuable talent from a serious character defect.

In severe cases of antisocial personality, individuals are likely to have a criminal record that clearly disqualifies them for access to classified information. They are also unlikely to have the history of academic or career success that qualifies them to apply for a position of responsibility. Moderately antisocial personalities, however, may appear to be very desirable candidates for employment. Such candidates are able to manipulate people so effectively that they do exceptionally well in interviews and are evaluated favorably by casual acquaintances. Their true character is revealed only after prolonged or intimate contact.

If a series of incidents shows a pattern of untrustworthy and unreliable behavior, it may not qualify as a psychological "disorder," but it may be adjudicated adversely under the Personal Conduct guideline or be considered as part of the whole-person evaluation under any other adjudicative guideline.

Antisocial behavior usually begins in childhood or adolescence. The most flagrant antisocial behavior may diminish after age 30. However, inability to sustain lasting, close, and responsible relationships with family, friends, sexual partners, or employer may persist into late adult life. [3](#)

Example: John Walker

As a youth, Navy spy John Walker rolled used tires down hills at cars passing below, threw rocks through school windows, stole money from purses and coats left unattended at school functions, stole coins from church donation boxes for the poor, set fires, and shot at the headlights of cars. When arrested for attempted burglary at age 17, Walker admitted to six other burglaries. He was pardoned on condition that he follow through on his plan to join the Navy. A childhood friend, who says he knew Walker like a brother, described him many years later as "cunning, intelligent, clever, personable, and intrinsically evil."

After his arrest as a Soviet spy, he enjoyed the publicity; he had no remorse. He rationalized involving his brother, son, and friend in espionage, and trying to recruit his daughter, as trying to help *them* be successful in life. He later criticized *them* for using *him*. He felt his only real mistake was allowing himself to be surrounded by weaker people who eventually brought him down. He concluded, "I am the real victim in this entire unpleasant episode."

One author who spent about 160 hours interviewing Walker after his conviction wrote: "He is totally without principle. There was no right or wrong, no morality or immorality, in his eyes. There were only his own wants, his own needs, whatever those might be at the moment." He

betrayed his country, crippled his wife emotionally, corrupted his children, and manipulated his friends. Yet all the while, he didn't see himself as different from others, only a little smarter. In his view, "Everyone is corrupt...everyone has a scam." [4](#)

Narcissism/Grandiosity

A narcissistic personality is characterized by unwarranted feelings of self-importance or self-esteem (grandiosity), a sense of entitlement, and a lack of empathy for others. These characteristics are discussed separately below and then related to security issues.

Grandiosity

Wholly unwarranted feelings of self-importance or self-esteem are referred to by psychologists as grandiosity. Grandiose persons grossly overestimate their abilities and inflate their accomplishments. They are often preoccupied with fantasies of success, power, beauty, or love. They may need constant reinforcement of this fantasy image of themselves. Grandiose persons expect to be viewed as "special" even without appropriate accomplishments.

Need for praise and sensitivity to criticism dominate relationships with others. Personal friendships, relationships with supervisors and coworkers, and amorous relationships turn quickly from love to hate, and vice versa, depending upon whether the relationship supports or undermines subject's self-esteem. The narcissist demands unconditional acceptance of his or her specialness, and relationships blossom only when this is given, and sour quickly when it is not.

Self-esteem is almost always fragile. An unreasonably high, overt self-evaluation masks inner doubts and insecurities. It is paradoxical that someone with such a crippling sense of inadequacy should act in such an arrogant, imperious, and grandiloquent manner.

Grandiose persons feel they are so smart or so important that the rules, which were made for ordinary people, do not apply to them. Rules and social values are not necessarily rejected as they are by the antisocial personality; it is just that one feels above the rules.

Entitlement

A sense of entitlement is characterized by *unreasonable* expectation of especially favorable treatment. Such persons expect to be given whatever they want or feel they need.

They may feel entitled to a promotion or to a higher grade in school just because they worked hard for it, regardless of the quality of their

performance; entitled to more money because housing or college costs are so high, even though they did not earn it; entitled to cut in front of the line because they are so busy or their time is so valuable. They may also feel entitled to punish others, to "give them what they deserve," because others failed to recognize their special abilities or frustrated their desires in some other way.

Instead of congratulating a colleague who receives a promotion, the narcissist may feel bitter and grouse that the promotion wasn't deserved. Several persons arrested for embezzlement have revealed that they started to take money only after someone on a par with them got a promotion that they did not receive. They felt entitled to take the money because they too should have been promoted.

Many people genuinely do get a raw deal, and may be justified in feeling they deserve better. Feelings of entitlement in such cases become a security problem only if the person is planning revenge or retaliation.

Lack of Empathy

Narcissists generally view the world from the perspective of how it affects them, and them only. There is little empathy or ability to understand the feelings or problems of others. For example, when a coworker becomes seriously ill, a narcissist may be upset by the inconvenience caused by the worker's absence and relatively unconcerned about the welfare of the worker.

Narcissistic persons shamelessly take others for granted and manipulate or exploit them to achieve their own ends. They may be unusually aggressive and ambitious in seeking relationships with others in positions of power. In romantic relationships, the partner is often treated as an object to be used to bolster one's self-esteem.

In extreme cases, the narcissist who gains power over others, as in a relationship between supervisor and subordinate, may use this power in humiliating and cruel ways, sometimes just for what seems like personal amusement. [3](#)

Relevance to Security

Narcissism should not be confused with the simple egotism found in many capable and loyal employees who progress to senior positions due to their strong abilities, self-confidence, and ambition. An unwarranted sense of self-importance is a concern only when self-evaluation is so far out of line with reality, and with how one is perceived by supervisors and colleagues, that disappointment and resentment are inevitable.

The narcissist's need for recognition is so strong that failure provokes a need for vindication and revenge. The compelling need to justify unwarranted self-esteem may cause a grandiose person with a grudge to seek recognition elsewhere -- with an opposition intelligence service or business competitor.

Feelings of entitlement are a security concern because they may be used to rationalize illegal behavior or may reduce the inhibitions that otherwise deter illegal behavior. When combined with antisocial attitudes, grandiosity, or desperate need or greed for money, a feeling of entitlement leads to easy rationalization of theft, fraud, or other illegal activity for monetary gain. "I'm only taking what I deserve." It is also an easy rationalization for revenge. "If they hadn't screwed me, I wouldn't be doing this, so it's their fault; they deserve it."

When narcissists fail to perform adequately at work, it is always someone else's fault. The many arrested spies who exhibited this characteristic blamed others for their treason. They blamed their behavior on the counterculture movement of the 1960s, on an insensitive and intrusive Intelligence Community, poor security practices, supervisors who failed to recognize their potential, spouses for not being understanding, or government for not taking the right political stance. Few saw themselves as traitors; they saw themselves as victims.

Self-deception and rationalization facilitate criminal behavior, as they enable an individual to consider such behavior in a more justifiable light. They also soothe an offender's conscience as the activity progresses. Narcissism is illustrated by the following example.

Example: Jonathan Pollard

Jonathan Jay Pollard was a Naval Intelligence analyst arrested for espionage on behalf of Israel. From an early age, Pollard had a fantasy of himself as a master strategist and a superhero defending Israel from its enemies. He became obsessed with the threats facing Israel and a desire to serve that country.

In college, Pollard boasted that he had dual citizenship and was a Colonel in the Israeli Army. His Stanford senior yearbook photo listed him as "Colonel" Pollard, and he reportedly convinced almost everyone that Israeli Intelligence was paying his tuition. After his arrest, Pollard said this was all "fun and games," and "no one took it seriously." But most of his fellow students did not see it as a game.

Pollard kept his pro-Israeli views to himself while working for Naval Intelligence, but other tall tales about himself were more or less a joke in the office. He was unpopular among his colleagues, as they resented his bragging, his arrogance, and his know-it-all attitude.

At one point, Pollard received permission to establish a back-channel contact with South African Intelligence through a South African friend he had known in graduate school. Through a combination of circumstances, Pollard's story about his relationship with the South Africans began to unravel. After telling Navy investigators fantastic tales about having lived in South Africa and his father having been CIA Station Chief there, Pollard's security clearance was pulled and he was told to obtain psychiatric help. When the doctor concluded he was not mentally ill, Pollard filed a formal grievance and got his clearance and job back.

Pollard's need to feel important, and to have others validate that importance, led him to pass several classified political and economic analyses to three different friends whom he felt could use the information in their business. This was before he volunteered his services to Israel. Although he hoped to eventually get something in return, his principal motive was simply to impress his friends with his knowledge and the importance of his work.

Several years later, under a different supervisor, it was again Pollard's grandiosity that attracted adverse attention, contributing to his eventual compromise and arrest. The supervisor caught Pollard lying about his dealings with another government agency. The only purpose of the lie was apparently to make Pollard appear to be a more important person than he was.

The supervisor wondered why Pollard would make up stories like this and began paying much closer attention to Pollard's activities. He noticed that Pollard was requesting so many Top Secret documents concerning Soviet equipment being supplied to the Arab world that it was becoming a burden on the clerk who had to log them in. What triggered the espionage investigation leading to Pollard's arrest was a report by a coworker who observed Pollard leaving the office at 4:30 on a Friday afternoon with a wrapped package of classified material and then getting into a car with his wife.

The risk Pollard ran by requesting so many documents may also be explained by his grandiosity; grandiose persons often think they are too smart to be caught. [5](#)

Impulsiveness/Immaturity

Impulsive and immature individuals lack self-control. They are a security concern because they may use poor judgment or be irresponsible or unpredictable in their behavior. A person who is impulsive or immature should usually also be assessed under the Personal Conduct guideline, as a pattern of dishonest, unreliable or rule-breaking behavior. Self-control, which is the opposite of impulsiveness or immaturity, is a favorable trait that may offset a variety of personal weaknesses.

Many of the immature, young military personnel who have volunteered their services to foreign intelligence services reported afterwards that they made an impulsive decision without thinking through the potential consequences. They did whatever gave them satisfaction or seemed to solve their financial problems at the moment, without considering the long-term effects on themselves or others.

Impulsive persons are motivated by the quick, easy gratification of desires and fail to consider the consequences of their actions. Goals or gains that can be achieved quickly are overvalued, while those that are more distant are undervalued. When a younger person exhibits this pattern, it is often described as immaturity.

Impulsive individuals may not be concerned about duties and obligations and may be careless or lazy. They cannot tolerate boredom and often require constant stimulation. Inability to tolerate frustration may lead to a sudden outburst of hostility or violence.

Immaturity is also characterized by propensity to take risks, susceptibility to peer pressure, and belief that one is invincible so nothing bad could happen. Although immature persons may be ambitious, they seldom appreciate the connection between current performance and long-term rewards. Excessive fascination with intrigue and clandestine intelligence tradecraft may be a sign of immaturity.

One of the prominent current theories of criminality argues that low self-control is the *only* personal characteristic that differentiates offenders from nonoffenders. According to this view, the necessary conditions for criminal acts are too little self-restraint and a desirable and conveniently accessible target. [6](#) Other persuasive theories of criminality focus on a wider range of social, biological and psychological variables.

Impulsiveness/immaturity and antisocial tendencies are a volatile mix. When combined with resentment, a desire for revenge, or judgment clouded by alcohol abuse, they comprise a recipe for trouble.

Example: Robert Hanssen

FBI Special Agent Robert Hanssen spied for the Russians for over 20 years until his arrest in 2001. Although he was quiet and withdrawn both at home and at work, childhood friends described Hanssen's behavior as sporadically impulsive and immature. One friend noted, "When he got an idea to do something enormously risky, there was no stopping him." During his teenage years, such risks included reckless shooting and irresponsible driving. Once, while shooting at targets in a friend's basement, he suddenly began shooting at the wall as his friends watched in amazement. Frequently, he liked to scare his friends with erratic, fast, and reckless driving. He would challenge friends to street races on narrow, winding roads, or try to find the maximum

speed his small car could reach while turning corners. His friends noted that he never warned them or asked them before he took off on an erratic driving spree, and that they often feared for their safety.

Hanssen's impulsivity and lack of self-control continued into his adult years, where it took on a more sexual nature. Within days of his marriage to his wife, he cheated on her with an ex-girlfriend. Twice during the early years of his marriage, he snuck up on his sister-in-law and touched her breast while she was breastfeeding, prompting suspicion from many of his relatives. He also liked to post erotic stories about himself and his wife on web sites, risking identification by using their real names and real situations. His most disturbing sexual adventure, unbeknownst to his wife, was asking his best friend to watch them having sex through the window of their bedroom, and later, on closed circuit TV wired from the bedroom into his very own living room.

There is evidence that Hanssen's first deal to sell classified information to the Russians was impulsive as well. From childhood, Robert Hanssen had been enthralled with KGB spycraft and fascinated with the spy game in general. When he joined the FBI he was idealistic. He was ready to nab Russian spies in what seemed the most exciting job of his life, especially considering his knowledge and understanding of the KGB. Unfortunately, his idealistic start turned to sour disregard, and even disdain, for his fellow FBI agents when he thought they did not share his enthusiasm for thwarting Russian Intelligence activities in the United States.

Lack of support and enthusiasm from his colleagues left Hanssen reeling. It also sparked an old fantasy--to become the best spy the world had ever seen. Hanssen had access to classified information that he knew was useful to the KGB. His first transaction, unfortunately, was not as glorious and well thought out as he would have hoped. When his wife walked in on him in the aftermath of the trade and discovered his first act of espionage, Hanssen was forced to rethink his means of operation, and to become a much more careful spy.

During the 20 years that Hanssen worked as a spy for the KGB, his impulsive behavior affected his spycraft. He would often not show up for "drops" or cancel a transaction without cause. He insisted that the KGB do things his way or no way. He felt this put him a step ahead of the KGB and ensured his personal anonymity and security. He believed that his intellectual superiority to both his fellow FBI agents and to the KGB rendered him untouchable. Although he knew the great risk of his spying, he was confident that he was invincible. [7](#)

Inability to Form a Commitment

Inability to maintain healthy, long-term personal or work relationships is a serious security concern as it indicates a low capacity for loyalty. Because

emotional, mental, and personality disorders often become apparent through their impact on interpersonal relationships, inability to form a commitment is a surrogate measure for a wide variety of suitability and mental health issues. It is often found together with antisocial behavior and/or narcissism.

Inability to make a commitment is not identified by a single event, such as a divorce. It refers to a *pattern* of poor relationships and an aimless or erratic life style or work history. Employment history may show a pattern of frequent job changes without corresponding career advancement (e.g., three or more jobs in five years not explained by the nature of job or economic or seasonal fluctuation; walking off several jobs without other jobs in sight). Relationships tend to be one-sided and often last less than one year. There may be a history of unhappy love affairs. Marriages are often unstable. After divorce, there may be no continuing contact with children. Inability to form enduring emotional commitments is often traced to abuse or neglect, split loyalties, or broken allegiances during childhood or adolescence.

Persons who are *unable* to form a commitment should be distinguished from the socially withdrawn individual who remains alone by choice. Most Americans who have been arrested for espionage were not loners. They had greater than average need for the attention, approval, and admiration of others, but many were *unable* to sustain long-term relationships because their behavior engendered resentment among family, friends, and coworkers.

Example: Christopher Boyce

Christopher Boyce compromised highly sensitive communications satellite programs to the former Soviet Union. He had been a model youth -- president of his middle school class and an altar boy who aspired to a career in the priesthood. In high school in the 1960s during the Vietnam War, he became deeply disillusioned with his religion and with the U.S. Government. [8](#)

When Boyce was investigated and approved for special access program and cryptographic clearances at age 21, the only evidence of his inner turmoil was having dropped out of three colleges during the previous three years and holding six part-time jobs during the previous two years. Of the six positions, he left three positions without giving notice, being ineligible for rehire at one of them, eligible for rehire at the second, and questionable for rehire at the third. A former landlord indicated he failed to take care of his apartment and moved without notice. He was described as young, immature and unsettled, and his friends in his last college town were considered "hippies." His then-current supervisor questioned his abilities and initiative and said he showed up for work on Mondays with a hangover. [9](#)

This information might have indicated to an astute observer that Boyce was not the type of person one could count on to make any form of long-term commitment involving access to some of the nation's most sensitive secrets.

Vindictiveness

Desire for revenge can trigger sabotage, espionage, violent attack, or other illegal behavior. Several well-known spies are known to have had a strong propensity toward vindictiveness.

Vindictiveness is often found in narcissists whose self-esteem is based on a grossly inflated opinion of their own abilities. They interpret criticism, disagreement, or failure to recognize their special talents as a personal insult that merits retribution. The retribution is a means of restoring injured self-esteem.

Vindictive behavior should be reported. Implied threats of vindictive behavior should be taken seriously. They merit management attention and careful security evaluation. This includes statements such as "You haven't seen the last of me; I'll be back." "I'll get even for that." "They can't treat me like that and get away with it." "Don't worry, I'll find my own way to get what they owe me." "If he does that one more time I'll..." Even if the individual *seems* to be just blowing off steam, such statements indicate a level of frustration that should be dealt with proactively. Review of security and personnel files by a mental health professional may be an appropriate first step in some cases.

Example: John Walker

Navy spy John Walker's daughter reported that he had books on revenge and on dirty tricks, such as putting epoxy glue into locks of cars and homes. Walker once told a friend: "You never confront a person face to face. You get even. Maybe three years from now." [10](#)

Paranoia

The paranoid personality is distinguished by a pervasive distrust and suspicion of other people. Such persons are preoccupied with unjustified doubts about the loyalty or trustworthiness of friends or associates. They are reluctant to confide in others for fear that information they share will be used against them. They may refuse to answer personal questions, saying the information is "nobody's business." They read hidden meanings that are demeaning or threatening into innocent remarks or unrelated events. They may interpret an innocent mistake by a store clerk as a deliberate attempt to shortchange them.

A supervisor's compliment on an accomplishment may be misinterpreted as an attempt to coerce more or better performance. An offer of help may be viewed as a criticism that the person is not doing well enough on his or her own. Minor slights arouse major hostility, and these slights are never forgiven or forgotten. Such persons often have unjustified suspicions that

their spouse or sexual partner is unfaithful. They want to maintain complete control over intimate relationships to avoid being betrayed. They may gather trivial and circumstantial "evidence" to support their jealous beliefs.

Paranoid personalities may blame others for their own shortcomings. Because they are quick to counterattack in response to perceived threats, they may become involved in legal disputes. Such persons are attracted to simplistic black-and-white explanations of events, and are often wary of ambiguous situations. Paranoia often disrupts relationships with supervisors and coworkers. Severe paranoia is often a precursor of other mental disorders or found together with other disorders. [3](#)

Paranoia is a serious security concern, as the paranoid can easily view his or her employer or the U.S. Government as the enemy, and act accordingly. Alternatively, what appears to be paranoia may have a factual basis. Seemingly extreme concern about being investigated or watched or searching for listening devices or hidden cameras may indicate that a person is engaged in illegal activity and fears detection.

Risk-Seeking

Risk-seeking is one particularly significant form of impulsive, irresponsible behavior. Risk-seekers ignore or gloss over risks (impulsiveness or immaturity) or think the risks do not apply to them because they are so clever or talented (grandiosity). They are inclined to become involved in reckless driving, gambling, fighting, vandalism, use of drugs such as LSD and PCP, holding up the local 7-11 convenience store, or becoming a spy.

When risk-seeking is combined with other weaknesses such as antisocial attitudes and inability to make a commitment, it may contribute to illegal behavior. Such persons may be attracted by the excitement of espionage rather than repelled by the risk. Examples from actual espionage cases are discussed below.

Risk-seekers often consider conventional lifestyles beneath them. They are restless and impetuous and cannot tolerate boredom or inactivity. Since work is not always exciting, they find it hard to sustain consistent work behavior.

This type of person cannot turn down a dare. They may think it is fun to see how close they can come to breaking the rules without getting caught. Sex is often just another way of getting kicks, so it is impersonal and devoid of emotional attachment.

It is important to distinguish thoughtless risk from calculated risk. Persons involved in the riskier hobbies or occupations, such as a mountain climber, downhill ski racer, sky diver, or military specialties such as fighter pilot undergo considerable training. They learn to control their nerves and emotions, carefully calculate the level of risk, and take appropriate

precautions to reduce the chances of adverse consequences. This is, in fact, good training in self-control.

Example: Aldrich Ames

In his CIA work, Aldrich Ames demonstrated the inconsistent performance typical of many thrill-seekers. He displayed what the CIA Inspector General's report on this case called "selective enthusiasm." According to this report: "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."

In his espionage activity, Aldrich Ames ignored risks by conspicuous spending of his illegal income, carrying large packages of money across international borders, and leaving evidence of his espionage on his home computer and hidden elsewhere in his home. [11](#)

Example: John Walker

Navy spy John Walker had a legendary reputation as a daredevil. For example, one night when returning to his submarine after some heavy drinking, he spotted a blimp tethered nearby. He led his colleagues in an effort to cut the blimp loose, but was scared off when a policeman shouted a warning and then fired a warning shot. [10](#)

Footnotes

1. Several government agencies have conducted comprehensive psychological assessments of their employees arrested for espionage, and an Intelligence Community project has interviewed and administered psychological tests to a number of Americans serving jail terms for espionage. Most interviews and tests were conducted after conviction and incarceration and were subject to agreements that protect the privacy of the offenders. Privacy and security considerations preclude public release of these studies.

2. Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press. Parker, J.P., & Wiskoff, M.F. (1992). *Temperament constructs related to betrayal of trust* (Technical Report 92-002). Monterey, CA: Defense Personnel Security Research Center. Collins, J.M., & Schmidt, F.L. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, *46*, 295-311. Brodsky, S.L., & Smitherman, H.O. (1983). *Handbook of scales for research in crime and delinquency*. New York: Plenum Press. Hogan, R., & Hogan, J. (1989). How to measure employee reliability. *Journal of Applied Psychology*, *74*, 273-279. Collins, J.M., & Muchinsky, P.M. (1994). Fraud in the executive offices: Personality differentiation of white collar criminality among managers. Paper

presented at 23rd International Congress of Applied Psychology, Madrid, Spain.

3. American Psychiatric Association. (1995). *Diagnostic and statistical manual of mental disorders* (4th ed.) (DSM-IV). Washington, DC: Author.
4. Kneece, J. (1986). *Family treason: The Walker spy case*. Briarcliff Manor, NY: Stein & Day. And Earley, P. (1988). *Family of spies: Inside the John Walker spy ring*. New York: Bantam Books.
5. Blitzer, W. (1989). *Territory of lies: The rise, fall, and betrayal of Jonathan Jay Pollard*. New York: Harper & Row.
6. Gottfredson, M.R., & Hirschi, T. (1990). *A general theory of crime*. Stanford, CA: Stanford University Press.
7. Vise, D.A. (2002). *The bureau and the mole: The unmasking of Robert Philip Hanssen, the most dangerous double agent in FBI history*. New York, NY: Grove Press.
8. Lindsey, R. (1980). *The falcon and the snowman*. New York: Pocket Books.
9. Declassified extracts from preemployment security investigation of Christopher Boyce.
10. Kneece, J. (1986). *Family treason: The Walker spy case*. Briarcliff Manor, NY: Stein & Day.
11. *Unclassified Abstract of the CIA Inspector General's Report on the Aldrich H. Ames Case*.

One Country's Program To Obtain U.S. S&T Secrets

This is an account of how a country we call Technomia organizes and manages a large program to obtain scientific and technological secrets from the United States and other advanced countries. Technomia is a fictitious name for a real country that is a friend and ally of the United States, not an adversary. As is true with a number of friends and allies, however, its high-tech industries do compete with the United States and others in the global marketplace.

The country name is changed here in order to avoid an inappropriate focus of attention on this single country. Technomia's systematic program to acquire

U.S. science and technology by illegal as well as legal means differs little from what is being done by a group of other countries, both allies and potential adversaries, that are also pushing the development of high technology as a national goal. Almost 100 countries are known to engage in some type of intelligence collection against U.S. technology.

This is an abridged version, with country name deleted, of unclassified reports published by the National Counterintelligence Center and its successor, the Office of the National Counterintelligence Executive.¹ The reports were based on a collection of 44 newspaper articles that appeared in the Technomian media during the period 1994-2001. The intended audience for the media articles was obviously the citizens of Technomia, not U.S. intelligence and security agencies. However, we have also learned from these articles, and there are lessons here for all individuals who are responsible for protecting U.S. classified, export-controlled, and proprietary information.

The principal lesson is that we should not underestimate the frequency with which technical personnel and scientists with foreign backgrounds are confronted with a choice between protecting classified or other sensitive information and providing that information to another country or individual to whom they feel some degree of loyalty or obligation.

In the mid-1990s, Technomian media began reporting that, over the previous two years the Technomia Government and Technomian companies have been engaging in systematic efforts to obtain foreign proprietary technology through "indirect methods." Faced with a decline in the competitiveness of its products, the high cost of buying foreign technology, and the difficulty of developing new technology through its own resources, Technomia contrived a number of alternative methods for obtaining access to the technological secrets of more advanced countries.

According to Technomian press reports, these techniques ranged from the exploitation of academic exchange programs to use of the country's intelligence service for industrial espionage. Several of these programs for acquiring U.S. technology reportedly targeted U.S. citizens through databases of information on former Technomian citizens now living in the United States. Many such initiatives reportedly were designed and managed by the Technomia Government itself. The press reports described a number of Technomia's methods for obtaining foreign technology, particularly from U.S. companies.

Despite its efforts, Technomia continued to suffer economic difficulties during the mid-1990s. As part of its uphill struggle to break out of its economic doldrums, Technomia increased its efforts to obtain foreign proprietary technology, according to Technomia media reports. Mechanisms through which enhanced collection activity was reported included "joint research," recruitment of foreign nationals, outposts located in high-tech regions abroad, expatriate scientists, and the National Intelligence Service's

apparatus. In addition, the Technomian Government reportedly formed a new committee to systematize foreign technology collection and expand the number of overseas collectors.

According to the press reports, the most-wanted technologies sought from the United States by Technomian companies and government research institutes were aerospace, automobiles, bioengineering, computers, communications, electronics, environmental, machinery and metals, medical equipment, nuclear power, and semiconductors.

Technomia's national laboratories were tasked by the government to "help domestic industry overcome the economic crisis" by rendering "practical" support for new product development and by "internationalizing their research activities." Examples of the latter included the Technomia Institute of Science and Technology (part of the Ministry of Science and Technology) program to "conduct personnel exchanges, information interchange, and joint research with 57 institutions in 19 countries." The Technomian Institute of Machinery and Metals (another affiliate of the Ministry of Science and Technology) planned to set up joint R&D centers at Stanford University and MIT to "acquire leading future technologies." Technomia also sought to expand these "cooperative exchanges" across a wide range of "state-of-the-art technologies."

Other countries also were increasingly targeted as sources of new technology. Technomian science officers stationed at 10 Technomia Government-funded research centers in Europe and Russia met to discuss ways to boost their research activity, described by one officer as the "systematic gathering of information on [host country] research institutes, technologies, and personnel."

Direct exploitation of overseas scientists by Technomia Government institutions was being enhanced by expanding the "brain pool" project according to an Internet posting by the Technomia-American Scientists and Engineers Association. Administered by the Ministry of Science and Technology and executed by the General Federation of Technomian Science and Technology Organizations through its chapters in eight foreign countries, the brain pool project offers salaries and expenses to "outstanding scientists and engineers from overseas" to share their knowledge in "all fields of science and technology" with their counterparts at Technomia national and corporate laboratories. In previous years, the notices capped the number of positions to a few dozen, whereas in 1998, the solicitation appeared to be open-ended.

Technomia companies likewise were increasingly eager to tap the expertise of foreign scientists. Subsidiaries of the country's major corporations "launched aggressive 'head hunting' operations" overseas aimed at scientists and engineers in electronics and information science. Several companies reportedly held briefing sessions and recruitment exhibitions "at major

universities and research institutes in the United States and Europe." One company, in particular, was "securing competent employees overseas by using Technomian students studying abroad on company scholarships, its overseas branches, and its own research institutes established in the United States as an information network. The overseas recruitment of scientific talent was being pursued by the large corporations and focused not only on established scientists but also on new graduates of prestigious U.S. technical universities.

Besides these company-led efforts, Technomians were establishing independent "consulting firms" overseas whose function is to "scout out technical manpower for Technomian companies" and broker the transfer of "core technologies" to Technomia producers. One such company reportedly was established in Moscow by "specialists engaged in technology transfers from Russia on behalf of large Technomian businesses." Another Technomian consulting firm opened offices in Los Angeles to "recruit high-tech personnel in data communications." A personnel officer from a Technomia company stated that fees of \$100,000 are not considered excessive for the services of a top foreign scientist and speculated that "hiring advanced specialists from foreign countries" would increase.

In the United States, Silicon Valley is a favorite venue for informal technology transfers through Technomia Government-backed outposts for marketing and "information exchange." According to a Ministry of Information and Communications press release of 17 November 1997, Technomia was funding the creation of "incubators" in Silicon Valley designed both to promote the sale of Technomia software products and conduct "technology exchange activities."

The Technomia telecommunications company was to create a capital fund with Technomia communications equipment manufacturers to support Silicon Valley-based American venture enterprises in advanced data communications. The Technomia Advanced Institute of Science and Technology funded the establishment of a semiconductor equipment-manufacturing firm in Silicon Valley, which is run by expatriate Technomians. The firm reportedly is designed to allow Technomia graduate students "to acquire technology at the same time they earn dollars" by performing research with world-class engineers.

Coordinating S&T collection efforts and integrating collection targets with the needs of Technomia manufacturers -- long a bottleneck in Technomia's informal technology transfer programs -- entered a new dimension as a result of programs undertaken by the Ministry of Science and Technology's Science and Technology Policy Institute. According to a report released by this institute on 9 December 1998, and cited by the Technomian press, the separate collection programs run by the Ministries of Foreign Affairs, Trade and Industry, National Defense, and Science are to be brought together under a "Science and Technology Foreign Cooperation Committee" meant to

systematize collection strategy, integrate local operations, and avoid duplication of effort. The committee reportedly would be divided into groups of specialists by geographical region who would interact with a council composed of working-level personnel from organizations such as the Technomia Trade Promotion Agency and the Science and Technology Policy Institute on the one hand, and national labs, universities, and Technomia companies on the other.

Reportedly formed to counter the "increasing reluctance of advanced countries to transfer their science and technology," the program entails establishing local "Technomia Centers" to collect foreign S&T information and to set up overseas branches of government bodies, national labs, and companies "to provide information on foreign S&T." Moreover, to "strengthen overseas S&T collection" and build an information system that would link Technomia organizations to overseas sources of technology, the Science and Technology Policy Institute was to create an "Overseas Science and Technology Information Center" that integrates the S&T information collected by "overseas associations of Technomian scientists and engineers, Technomian diplomatic and consular offices in foreign countries, large Technomian trading companies, and the overseas offices of national labs."

The Technomian-U.S. Science Cooperation Center, a Technomia Government-funded S&T collection facility and host to the Technomian-American Science and Engineers Association, is now well established. Items posted on its Internet Web site included an invitation for proposals to create new programs designed to promote S&T cooperation and to help "Technomian and American scientists develop and maintain permanent S&T networks."

The Technomian Government is continuing its efforts to recruit ethnic Technomian scientists abroad to support state and corporate-defined research programs, as evidenced by a Science Ministry posting that called for a transnational "brain pool." The pragmatic nature of these efforts was brought out in the posting, which emphasized the importance of making concrete contributions to the country's S&T agenda.

According to a notice posted in April 2001 on the Technomian Science Ministry's Web site, the ministry, in conjunction with liaison organizations, renewed its sponsorship of the "brain pool" project to recruit foreign technical specialists willing to share their accumulated expertise with Technomia. The notice read in part:

The General Federation of Technomian S&T Organizations, in accordance with the government's (Ministry of Science and Technology) plan to recruit and make use of high-level overseas scientists (brain pool), is seeking world-class superior overseas scientists and engineers willing to contribute to raising our country's international competitiveness for on-site work at colleges,

companies, and Technomian R&D facilities. We hope for your wide participation.

The notice invited overseas scientists with recognized skills in areas "targeted for national strategic development" to apply. Some 30 different fields were listed, ranging from basic science to applied technology. Employment reportedly involved working with an existing R&D team or one formed around the scientist's area of expertise. Lecturing at seminars and before "scholarly associations" is also an option. Appointments ranged from three months to two years.

The ministry advised that applicants should be "overseas Technomian or foreign scientists and engineers" with more than five years postdoctoral experience in a foreign country. However, exceptions would be made for those who demonstrated outstanding research ability or who "possess know-how."

Periodic reporting in the Technomia media on the development of these programs has continued at least through 2003.

Footnote

1. National Counterintelligence Executive (n.d.) *CI History* (Vol. 4, Chap. 3). Retrieved February 15, 2006, from <http://www.ncix.gov/history/index.html>

In the Line of Fire: American Travelers Abroad

While traveling abroad, Americans are on the other country's home turf, where the local security and intelligence services have many resources available. They can monitor and, to some extent, control the environment in which Americans live and work. Any American government official, scientist, or business traveler with access to useful information can become a target of the local intelligence or security service in almost any country.

Some of the intelligence activities directed against Americans traveling or stationed abroad are quite sophisticated and unlikely to be noticed or identified for what they are. Others may be crude and obvious, like most of those described below.

This article consists of a series of anecdotes about foreign intelligence activities observed by travelers from the Department of Energy's Lawrence Livermore, Los Alamos, Sandia, and Oak Ridge National Laboratories. Most of the travelers were scientists traveling overseas on official business to attend meetings and conferences and to perform research. Many were traveling in

countries that place a high priority on collecting information about U.S. technology. [1](#)

The U.S. Government, as a matter of policy, does not identify publicly those foreign countries which represent the greatest intelligence threat. The reality is that most technologically advanced or developing countries, including some democratic countries that are closely allied with or supported by the United States, place a high priority on acquiring U.S. technology by both fair means and foul.

Anecdotes

The anecdotes below are a typical sample of observations reported over, and over, and over again by government, business, scientific, and academic travelers. In some countries, such happenings are rather normal, not exceptional. All personnel who experience such activities are supposed to report this to their security office, so that security personnel can keep abreast of what is happening and warn other travelers. This type of experience should also be reported during the personnel security investigation even if the subject has previously reported it to his or her security office.

- A traveler in a U.S. delegation said that before the start of one of its meetings, the delegation met in private to discuss talking points, negotiation strategies, and issues it wanted to avoid with its hosts. When the meetings began, the host country chairman began his opening remarks and listed almost point-by-point each of the issues that the delegation had discussed. Because no host country nationals had been privy to the delegation's discussions, the traveler was convinced that the discussions must have been monitored.
- A traveler awoke in his hotel room and realized he was late for a meeting with his team members. On the way out of his room, he saw an unidentified male standing in the open doorway of a team member's room. The male turned toward the traveler and said something in the native language to someone else in the room. Immediately, a woman stepped out of the room and into the hall. Both individuals appeared very surprised and nervous about being discovered. The traveler relayed this incident to the team, none of whom had experienced any problems. The team member whose room had been entered possessed all the financial data that the U.S. team was going to use in the negotiations. The host country would be very interested in obtaining that information.
- A traveler attending a workshop returned to his hotel room after being away for dinner. He went to bed and was awakened six hours later by a beeping noise. The noise was coming from the traveler's laptop computer. The computer cover was closed, but the unit was not shut off. The traveler believes that while he was out of the room, the

room was searched and the laptop was opened and inspected but not turned off. This caused the battery to run down, which is what had caused the beeping. The traveler had not turned on the computer during his trip. No classified, sensitive, or proprietary information was on the computer's hard drive. On the last night of the workshop, a banquet was held, and a considerable amount of alcohol was consumed by participants. However, one host country participant was observed to be drinking no more than an ounce or two all night. Later, this individual offered to provide a woman for the traveler and another colleague. Both declined.

- During a workshop, a traveler was approached by a host country national who addressed the traveler by name before the traveler had a chance to put on his name tag. Throughout this week of meetings, this individual was very attentive to the U.S. travelers. He was interested in learning about the traveler's laboratory address and how the traveler's organization in the laboratory was related to other laboratory programs.
- A traveler found four entries for "guest access" on his laptop computer. The computer had been locked with a commercially available padlock and left in his room unattended. It was not clear if someone had actually accessed any files on the hard drive. He then checked the computer's protection software and found another "guest entry" had been logged on. The date of this entry coincided with a previous trip the traveler took to the same country.
- A traveler telephoned his wife at home. During their conversation, his wife mentioned an upcoming bus trip that she would be taking and that they would be playing bingo on the bus. A short time later, someone mentioned to the traveler the bingo trip that his wife had talked about. The next day, another person asked, "What is bingo?"
- A traveler presented various lectures to university audiences and the general public throughout the country. Although the presentations were all unclassified, the traveler had to deflect several questions from host country nationals at each venue that touched on sensitive or classified information. At one lecture, he was asked questions about a specific nuclear isotope and its relation to U.S. nuclear devices.
- A traveler was propositioned by prostitutes every night. On the first night, he received a phone call from a prostitute within a few minutes of entering his hotel room. This was the case each night, and he did not think it was the same woman every night. He declined these offers. On one occasion, a prostitute knocked on his hotel door. The traveler said that there was a female "hall monitor" in the hotel. He believed that the monitor was providing surveillance for prostitutes.
- In a moment of frustration, a traveler mentioned to another traveler while in his hotel room that "any decent hotel would at least have a spare roll of toilet paper in each room." Later that day, upon

returning to the hotel room, the traveler noticed that there was an additional roll of toilet paper in his room. This and other unusual occurrences during the visit led the traveler to believe that audio surveillance was being utilized.

- While engaged in negotiations in another country, a laboratory team reported that the host nation participants were very forceful in trying to have a particular technology included in the contract's statement of work. This technology currently cannot be shared and thus was not included in the statement of work.
- A traveler noticed that his laptop computer had been tampered with while it was left unattended in the closet of his hotel room. When he turned on the computer, he noticed that someone had successfully bypassed and turned off the password protection. The battery compartment door on the underside of the computer was broken. The traveler reported that one of his colleagues had a similar problem with his laptop.
- A traveler reported that a colleague placed something in his suitcase that would alert him if the suitcase was searched during his absence. Later, the suitcase was searched, but nothing was taken from it.
- A traveler was invited to join a high-ranking official on a hunting trip for the weekend. The traveler told the official that he had been briefed and instructed to always bring along another team member when traveling in that country. The official told him he could bring along his host country's interpreter. The traveler did not go on the hunting trip.
- While staying at a guest house, a traveler placed his belongings on the shelves in the room. He carefully placed his business paperwork between various clothing items. Several hours later, when he returned to his room, he noticed that someone had gone through his papers, because they were out of order and sloppily put back in different places. Also, someone attempted to access his electronic organizer.
- A traveler was approached by an interpreter with questions about his personal life. The traveler was not comfortable with these questions and refused to answer them.
- A traveler suspected that the briefcase he had left in his hotel room had been tampered with. His briefcase, which he never locked during the trip, was found locked when he tried to open it. The briefcase contained nothing sensitive or classified, and nothing appeared to be missing.
- A traveler reported that the interpreter from the host country appeared to be compiling biographical information on him. The interpreter said that he recognized the traveler from an article in a trade magazine, which the traveler found unlikely.

- An individual who was not from the host country asked a traveler questions about his new work at his laboratory. The traveler was surprised by this question, because few people knew of his new assignment, and this was not related to the purpose of his travel. The traveler said that it seemed the individual was specifically assigned to him to elicit information. The traveler did not provide the requested information.
- A traveler experienced a burglary in his second-floor hotel room. The traveler's briefcase was taken, but other valuables, including money left next to the briefcase, were not taken. The briefcase contained documents with proprietary and sensitive information, the traveler's laboratory identification badge, and his office key. The briefcase was later recovered and returned to the traveler with all the contents intact by a host country colleague.
- A traveler at an international conference was approached by another participant who asked for a list of fission products. The traveler thought this participant was asking about fission products released from nuclear reactors and said these were available in the open literature. The participant then said that he wanted products from nuclear weapons. The traveler told him that he did not work in that area. The participant then asked for the names of people who do work in that area.
- At a meeting that was held in a hotel, housekeepers entered the conference room and rearranged some of the plants, placing one plant very close to the traveler and another U.S. laboratory colleague. Their host joked that they could not hear them well enough and so moved the plant closer. The traveler presumed that the plant contained a bug.
- It bears mentioning that the above anecdotes are known only because the foreign intelligence or security service made a mistake, such as leaving papers in a different order, locking a briefcase that the traveler did not lock, failing to turn off a laptop computer, etc. The frequency with which such activities are successful without leaving any evidence behind is, of course, unknown.

Footnote

1. All anecdotes are from United States General Accounting Office. (2000, June). *Department of Energy: National security controls over contractors traveling to foreign countries need strengthening* (GAO/RCED-00-140). Washington, DC: Author.

Potential CI Risk Indicators

Potential counterintelligence (CI) risk indicators are observable behaviors, conditions, or circumstances that are useful in assessing the risk that an individual may become, or may already be, involved in espionage or terrorism. This list and categorization of counterintelligence risk indicators is prepared for two purposes: (1) to assist training of personnel security investigators and adjudicators in the recognition of risk indicators and the assessment of counterintelligence risk, and (2) to assist in developing guidance for what actions should be taken when potential counterintelligence risk indicators are recognized or discovered at various stages of the personnel security process.

The personnel security investigation and subsequent adjudication provide an opportunity to identify and evaluate these indicators. As described here, there are three broad categories of potential CI risk indicators with multiple subcategories. 1

- Potential Indicators that the Subject May Be or Become a Target for Recruitment
 - o Circumstances Beyond the Subject's Control
 - o Behaviors that May Attract Foreign Intelligence Attention
 - o Indicators of Already Being a Target
- Potential Indicators of Susceptibility to Espionage or Terrorist Activity
 - o Indicators of Conflicting Interests
 - o Indicators of Vulnerability to Pressure or Duress
 - o Indicators of Competing Identities
 - o Indicators of Personal Weaknesses
- Potential Indicators of Espionage, Terrorism, or Subversive Activity
 - o Indicators of Recruitment
 - o Indicators of Information Collection
 - o Indicators of Information Transmittal
 - o Indicators of Illegal Income
 - o Indicators of Terrorist Activity
 - o Indicators of Support for Terrorism
 - o Other Behavioral Indicators

These are called “potential” indicators because no single indicator constitutes evidence of terrorism, espionage, or any other unauthorized use of classified or other protected information. Most counterintelligence risk indicators are what might be called “soft” indicators. That is, each indicator only tells us that something may happen or may already be happening, not that it will happen or actually is happening. Each specific behavior may have several possible explanations, and each particular condition or circumstance may have several possible outcomes. Therefore, most single indicators have limited significance. However, they alert the investigator or adjudicator that further inquiry may be appropriate to clarify the situation and determine if other indicators are also present.

The significance of any single indicator is greatly influenced by the presence of certain other indicators, and various combinations of indicators may form a pattern that is a valid basis for doubt or suspicion. Two types of interaction between risk indicators are especially important.

- An indicator that an individual may be a target for recruitment is far more significant if there is also some indication of susceptibility to recruitment, and either one or both of these enhance the significance of any indicator that this same individual may already be engaged in espionage or terrorism
- If an individual has family, friends, or professional associates in a foreign country, the significance of these foreign contacts is increased if there is also some indication of susceptibility to recruitment, and especially if there is any indicator that this individual may already be engaged in some improper activity.

The modus operandi for the recruitment of spies and the conduct of espionage often follows well-established patterns. These often make it possible for a counterintelligence specialist to recognize scenarios, or combinations of indicators, associated with foreign intelligence activity.

Use of CI Risk Indicators For Personnel Security Decisions

Evaluation of the possibility that an applicant for security clearance or a current clearance holder is now a foreign agent, or is at risk of later becoming a foreign agent, is a principal underlying purpose of the personnel security process. However, this is a difficult evaluation to make, and two significant problems arise when seeking to perform this function in the most efficient and effective manner.

- First, there are practical limits on the number of questions that can be asked during a standard personnel security subject interview, but an almost unlimited number of questions that might be relevant under various combinations of circumstances.
- Second, there are practical limits to the amount of counterintelligence knowledge and expertise that can be expected from the average personnel security investigator or adjudicator.

In order to deploy limited personnel security resources in the most effective manner, it would be helpful to have a system of triage to guide an optimal, risk-based allocation of resources to various types of cases. The comprehensive list of counterintelligence risk indicators in this report, broken down into analytically useful categories, may facilitate the development of such a system.

Decision points where counterintelligence indicators should play a role include the following:

- Review of the SF-86 to determine if a subject interview should be conducted in a NACLC investigation, whether an interim clearance should be granted, or if an investigator with counterintelligence training and experience should be assigned from the beginning to conduct expanded questioning.
- Review of the completed investigation to determine if a special interview should be conducted to cover Foreign Influence or counterintelligence issues, or if the case should be referred for counterintelligence review.
- Determine if further investigative action such as polygraph examination, check of bank or other financial records, or check of computer logs is appropriate.

Which action may be most appropriate in any given case depends upon the specific combination of indicators that are present. There is no national investigative standard that specifies what action is appropriate under which circumstances, and the Adjudicative Guidelines for Determining Eligibility for Access to Classified Information address counterintelligence issues only indirectly.

Potential Indicators of Being Or Becoming a Target for Recruitment

There are three types of indicators that an individual may become or is already a target for recruitment by a foreign intelligence collector. The first includes circumstances over which the individual has no control, but which make them an attractive target. The second is specific behaviors by the individual that may attract the attention of an intelligence collector and lead to the individual becoming a target. The third is circumstances that may indicate the individual already is a target.

A substantial percentage of cleared personnel are vulnerable to becoming a recruitment target through no fault of their own simply because of the nature of the information to which they have access, where they are stationed or travel, or their ethnic or cultural background. It is emphasized that being a recruitment target does not reflect poorly on the individual. It is very different from saying that an individual is susceptible to recruitment. However, just being a target for recruitment is a risk factor, because it increases the likelihood that any susceptibility to recruitment that does exist will be discovered by a foreign intelligence collector.

Circumstances Beyond the Subject's Control

One of the most important risk factors is the country in which the subject maintains contacts or where an individual is assigned or resides. Almost 100 countries were involved in legal and illegal efforts to collect intelligence in the United States during 2004, but the bulk of the activity originates in a relatively small number of key countries.² These key countries include friends and allies as well as strategic competitors that conduct a systematic program of espionage against the United States for one or more of the following reasons:

- The country competes with the United States for global or regional political and economic influence.
- The country feels threatened by a hostile neighbor and seeks to develop or obtain the most advanced military technology. It may also seek information on U.S. policy toward itself and the hostile neighbor, intelligence information the U.S. has on the hostile neighbor, and to influence U.S. policy toward itself and the hostile neighbor.
- The country has a developing economy and sees its economic future as being dependent upon the rapid acquisition and development of new technologies by every possible means, both legal or illegal.
- The country competes with U.S. companies in the global marketplace for the sale of advanced technologies or military weaponry.

Foreign intelligence collectors find it easier to contact, build rapport with, assess, and manipulate individuals with whom they share some common interest – including a shared national, ethnic, or religious background. Also, it is much easier for foreign intelligence collectors or terrorist groups to contact, assess, and recruit Americans when the American is in the intelligence collector's home country. Therefore, the following circumstances increase the likelihood that an individual will become a target.

- Relatives, friends, or business or professional associates in a foreign country that is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.
- Foreign relatives, friends, or business or professional associates who are aware that the subject has a security clearance for access to classified information.
- Foreign relatives, friends, or business or professional associates who have jobs or other activities that would make them very interested in the classified or other sensitive information to which the subject can gain access.
- Travel to or assignment in a foreign country that is known to target U.S. citizens to obtain protected information and/or is associated with a risk of terrorism.
- Employed in science or technology research and development with close or frequent contacts in the same field in a foreign country.

- Attendance at international conferences or trade shows. Many of these events, especially those dealing with science or technology, attract many intelligence collectors.
- Evidence that a foreign intelligence collector is targeting the specific technology to which the subject has access.
- Access to very sensitive information that is highly sought after. (Note: It is easy to overemphasize the extent to which the value of information available to an individual determines the chances of that individual being targeted. Foreign intelligence operatives are under pressure to recruit agents just as salesmen are under pressure to make sales. Their career advancement depends on it, but they also need to avoid getting caught. As a result, they often go after the easiest or most available target, rather than take the risk of going after the most valuable target. Support personnel such as secretaries, computer operators, and maintenance personnel can often provide access to very valuable information.)

Behaviors that Attract Foreign Attention

Some behaviors in a foreign country, or when interacting with foreign officials or other foreign nationals in the United States, are known to attract the interest of foreign intelligence collectors or terrorist groups. Again, the significance of most of these behaviors depends in part on the country involved. The significance is greater if the foreign country is known to target American citizens to obtain protected information and/or is associated with a risk of terrorism.

- Any action that draws the attention of a foreign security or intelligence service or terrorist group to an individual's ties of affection or obligation to a citizen of that foreign country. This includes regular telephone or e-mail contact with, sending packages or money to, or visiting a foreign relative, friend, or business associate. The more frequent and extensive the contact and the stronger the apparent ties of affection or obligation, the greater the chances that the contact will come to the attention of and be exploited by a foreign security or intelligence service or terrorist group.
- While traveling abroad, engaging in any activity that is illegal in the foreign country involved or that would be personally embarrassing if the activity were exposed. In many countries the local security service monitors patronage of prostitutes, homosexual bars, and the drug scene. In some countries black market currency exchange, distribution of religious information, and export of certain antiquities are illegal.
- Behavior while abroad or in the United States that is observable by a foreign national, especially by a foreign government official, and that shows strong disagreement with U.S. policy, anger at one's

employer, or an exploitable weakness such as a serious financial problem, an alcohol or gambling problem, drug use, or compulsive sexual needs.

- Foreign relatives or friends are made aware of the individual's access to classified or other protected information.

Indicators of Already Being a Target

It is not at all unusual for Americans traveling or living abroad to see signs of being cultivated, observed, or monitored by the local security or intelligence service. Indicators of being a target include the following:

- While traveling abroad, a foreign acquaintance seeks to elicit information about one's work, access to information, organization, or personal life. A new acquaintance shows knowledge about one's work or personal life that this individual would not be expected to know unless he or she had been briefed.
- A traveler observes indications of being followed, or that hotel room conversations, telephone conversations, or e-mail are being monitored.
- A traveler carrying sensitive government or business documents has his or her luggage or hotel room searched, papers or computer searched in the hotel room at night, or a briefcase or bag containing sensitive material is stolen.
- Unsolicited attention by a prostitute in the hotel where one is staying.
- Meeting a foreign national (often younger) who quickly becomes romantically infatuated with the (sometimes older) American.
- Request by a foreign national to provide unclassified information to help that person keep track of technology developments in the United States or keep up-to-date about U.S. policy.
- Travel to a foreign country that is paid for by someone other than family or employer, such as receiving an invitation to present a lecture or attend a conference in a foreign country at the expense of the host.
- An individual is contacted by a former coworker who has since been hired by a foreign controlled company.
- Receipt of an unsolicited e-mail request or "survey" from a foreign source requesting information about the individual's organization or area of expertise.
- An individual who is not looking for a job is contacted by a "head hunter" or other person seeking to interview the individual about an unsolicited job offer. Questions about the individual's job experience cannot be answered without divulging sensitive or proprietary information to what is essentially an unknown party.

- A foreign visitor to an organization attempts to meet and socialize with cleared personnel of the same ethnic or cultural background.
- A foreign national proposes that the individual work as a paid “consultant.”
- A foreign national hints that he or she may be able to help a relative or friend of the individual get a better apartment, job, or medical treatment.
- A foreign national hints that he or she may be able to help the individual financially – for example, finance research, pay for a child’s education, buy a new car, or pay family medical bills.
- A friend or acquaintance encourages the individual to live beyond his or her means, and then later offers to help the individual continue that lifestyle.
- A friend or acquaintance encourages the individual in their anger, resentment, or disgruntlement with their employer or opposition to U.S. Government policies, and then offers to help the individual get even with the employer or to oppose the objectionable policy.

Potential Indicators of Susceptibility To Espionage or Terrorist Activity

Susceptibility to espionage or terrorism includes both the susceptibility to being recruited by a foreign interest and susceptibility to volunteering one’s services to the foreign interest. (Most recruits are volunteers.) Susceptibility to recruitment also includes both susceptibility to inducements to cooperate and vulnerability to pressure or coercion. As with all indicators, their significance depends in large part on the foreign country involved. It is greater if the country is known to target aggressively American citizens to obtain protected information and/or is associated with a risk of terrorism. The significance of all foreign contacts also depends upon the closeness of the tie, frequency of the contact, and the occupation and interests of the foreign contact.

Indicators of Conflicting Interests

- Any evidence of divided loyalty between the United States and another country or organization.
- Any evidence of an obligation to another country, such as any exercise of a right or privilege of foreign citizenship.
- Individual responds, when asked, that he or she feels an obligation to assist the economic development of the native country, or the military defense of the native country against a hostile neighbor.
- Individual responds, when asked, that he or she may have a problem protecting information that would be of value to the native country but which the U.S. Government is unwilling to share. (This is

particularly significant if the individual may have access to such information, which includes much advanced technology and access to any of the large Intelligence Community networks that include intelligence reports on many different countries.)

- Individual responds, when asked, that family members or friends in the native country would be upset if they knew he or she is working on a Secret project for the U.S. Government or military. (This shows the kinds of people the subject associates with and that might influence the subject.)
- Repeated statements that raise questions about a person's loyalty to the United States, such as statements of support for actions by a foreign group hostile to U.S. interests. (This does not include legitimate dissent or disagreement with U.S. Government policies.)
- Statements that a person puts the interests of a foreign country, organization, or group ahead of the interests of the United States. For example: the person says he or she may be unable to support the United States in the event of a conflict with a specified country.
- Friends or relatives in the native country hold jobs or are involved in activities that would cause them to be very interested in the classified or other protected information to which the subject has access.
- For an individual with foreign business contacts, the success of a business transaction, and perhaps the individual's income or career, depends upon the good will of a foreign individual or entity.
- The individual considers his or her own classified research or development as his or her own personal property that may be shared with others.
- The individual is a scientist who believes that research findings should always be shared rather than protected.
- Any paid association with a foreign person or entity, especially if the association is unknown to one's employer or is with an organization that competes with one's employer.

Indicators of Vulnerability to Pressure or Duress

Most spies volunteer their services or are willing recruits, but aggressive foreign intelligence and security services do use pressure and duress when it serves their purposes. There are two general circumstances when an individual is vulnerable to pressure or duress. One is when an individual engages in conduct that, if exposed, could cause the person to have severe problems with spouse, family, or employer or adversely affect the person's personal, professional, or community standing. The other is the presence of a relative or friend in the foreign country whose life might be either improved

or made more difficult, depending upon whether or not the subject cooperates with the foreign intelligence or security service.

Even when an individual is vulnerable to pressure or duress, the foreign intelligence recruiter will usually try to avoid outright coercion whenever possible. Intelligence operatives understand human nature and know that a willing spy will be more effective and more trustworthy than one who is coerced to cooperate. A foreign intelligence or security service might first ask for cooperation and offer inducements rather than make threats. For example, it can make the life of the target's relative or friend better as well as worse, and it is more likely to be successful with the carrot than the stick. If the recruitment target is already fearful of what will happen if he or she refuses, explicit threats may be unnecessary.

Vulnerability to pressure or duress is difficult to assess, as the vulnerability exists in the mind of the individual concerned. Different individuals may react quite differently to the same circumstance. Many individuals who want to obtain or retain a security clearance will automatically answer no if asked whether a certain circumstance makes them vulnerable to coercion, as they recognize this might lead to denial of access to classified information. Some do, however, admit their vulnerability.

Indicators of vulnerability to pressure or duress include the following:

- An individual has a strong fear of the security service and what it might do to relatives or friends.
- An individual is easily influenced or compliant, unwilling to say "no," prefers to avoid conflict or confrontation.
- Relatives or a close friend or business contact in a foreign country may be helped if the individual agrees to provide information, but may be hurt if the individual refuses.
- Sexual behavior while living or traveling overseas that would cause severe embarrassment or other difficulties if it were exposed.
- For an immigrant to the United States, past receipt of any foreign government funding for the education in the United States or charitable assistance from a foreign organization in getting resettled in the United States. (Such assistance may create an obligation to the foreign country or organization.)
- Significant debt to a foreign government or foreign nationals, or foreign financial interests that could be affected by the foreign government.
- Any offense that is technically a crime in the foreign country, even if it is rarely prosecuted, such as currency exchange on the black market.
- Also see indicators listed above under *Behaviors that Attract Foreign Attention* and that might cause one to become an intelligence target.

Indicators of Competing Identities

Competing identities are defined as the dual self-identifications experienced by individuals who were raised as citizens of a foreign country but have since established their residence in the United States. Indicators are used to assess the degree to which the individual remains identified with his or her native country and the degree to which he or she has assimilated American culture and values. The focus here is only on indicators of continued identification with one's native country. A more complete list of such indicators is available in the reference. [3](#)

Many naturalized American citizens feel some degree of loyalty to both the United States and their native country, and most of the time this is not a problem. However, if an individual is motivated to help the economic development or military defense of his or her native country against a hostile neighbor, the two loyalties may conflict when that individual gains access to classified or other protected information of substantial value to the native country. This conflict can be exacerbated by a personal belief that the United States is wrong in not sharing this information. It could also be exacerbated by a financial need that could be satisfied by selling this information. Persons in this situation sometimes rationalize their actions as not being harmful to the United States.

An individual may continue to identify primarily with his or her native country if he or she:

- Came to the United States for educational or economic benefits rather than as political refugee or to be with family who had come previously to the United States.
- Was educated during the formative years at least through high school in the native country.
- Most of the individual's family remains in the native country.
- Communicates via telephone, e-mail, instant messaging, or mail with friends or relatives in the native country at least once every two weeks.
- Provides financial or other support, such as medicine, to relatives in the native country.
- Has expressed feelings of obligation to the native country.
- Did not apply for U.S. citizenship as soon as he or she was eligible.
- Views acquisition of American citizenship as a means to gain economic opportunities rather than as a commitment to American values and traditions.
- Is reluctant to give up a foreign passport or to renounce foreign citizenship.

- Maintains or will inherit investments, property, or other financial interests in the native country. Obtains income from the native country or is involved in a joint business venture there with a friend or relative.
- Returns to the native country annually.
- Resides in a culturally closed community with individuals from the same country of origin.
- Has a network of friends that consists largely of persons with the same national or ethnic background.
- After gaining U.S. citizenship, returned to native country to obtain a spouse and brought him or her back to the United States (or plans to do so).
- Frequently expresses a negative view of U.S. culture and values.
- Frequently expresses disagreement with U.S. policy toward the native country.
- Is actively involved in social or political organizations that support his or her native country.
- Contributes to charities in the native country or provides financial assistance to causes or individuals in that country.
- Makes references to wanting to return and live in the native country, for example, to retire there.
- Maintains regular communication with individuals in the native country who share the same professional interests and expertise.

Indicators of Personal Weaknesses

There is no single profile of the employee who is likely to betray an employer's trust. Motivation for espionage is believed to result from a complex interaction between personal weaknesses and situational circumstances. The personal weaknesses include some of the potentially disqualifying factors covered by the Adjudicative Guidelines, but also a number of personality characteristics that are often found in persons who commit espionage and other white-collar criminals.^{4,5} These same personality characteristics are also found to some degree in many law-abiding and successful individuals, so they are by no means disqualifying by themselves. These behaviors are discussed in greater detail in the separate file in this module on [Behavior Patterns and Personality Characteristics Associated with Espionage](#). The indicator always refers to a pattern of undesirable behavior, not a single example of such behavior.

- Antisocial behavior: involvement in petty crimes that indicate a propensity for violating commonly accepted rules and regulations, pattern of lying, misrepresentation, gross exaggeration, or failure to follow through on promises or commitments. Unscrupulous and has no conscience, so feels no remorse for the adverse effects of one's

behavior on others. Takes pleasure in beating the system and not getting caught, or cutting corners to achieve personal objectives.

- Impulsive: doing whatever feels good at the moment, without regard for duties or obligations, or without regard for the long-term consequences for self or others. Goals or gains that can be achieved quickly are overvalued, while those that are more distant are undervalued. When a younger person exhibits this pattern, it is often described as immaturity. Impulsive individuals may not be concerned about duties and obligations and may be careless or lazy. There may be a pattern of not completing tasks. Such persons cannot tolerate boredom and often require constant stimulation. Inability to tolerate frustration may lead to a sudden outburst of hostility or violence.
- Grandiosity: entirely unwarranted feelings of self-importance. The view of one's own abilities is so grossly inflated that disappointment and bitterness against those who fail to recognize these special talents are inevitable. Need for praise and sensitivity to criticism dominate relationships with others. Overreacting to criticism and responding with anger, even to constructive and well-intentioned criticism, is common. Fantasies of oneself as a James Bond, as indicated by repeated statements or actions indicating an abnormal fascination with "spy" work, can also be indicative of grandiosity.
- Narcissism: viewing the world only from the perspective of how it affects oneself. Narcissism often involves treating other people as objects to be manipulated for the benefit of one's own self-interest or to indulge one's own desires.
- Entitlement: unreasonable expectation of especially favorable treatment. Such persons expect to be given whatever they want or feel they need and become very upset when they don't get it.
- Vindictive: Such a serious grievance with one's boss, employer, or with the U.S. Government that the person has threatened violence or other vindictive action to get even. (Even if an individual seems to be just blowing off steam, all credible threats must be taken seriously.)
- Risk-seeking: taking risks just for the thrill of it without thinking of possible long-term consequences.
- Unable to make personal commitments: may drift from one relationship or job to another with little sense of purpose or loyalty to anyone or anything; limited capacity to express either positive or negative emotions towards others.
- Paranoid: pervasive mistrust and suspicion of other people. The security concern is that the paranoid person sometimes views his or her employer or the U.S. Government as the enemy and acts accordingly.
- Financial: Serious financial needs or excessive preoccupation with acquiring money or possessions. When financial need is triggered by a specific event such as divorce, medical expenses for a loved one,

educational expenses for children, large gambling losses, or threatened bankruptcy, it can cause one to reevaluate one's priorities and sometimes one's loyalties.

- Any exploitable weakness as identified under the Alcohol, Drugs, Crime, Sexual Behavior, and Personal Conduct adjudicative guidelines.
- Deliberate withholding or misrepresentation of information required on the personnel security form (SF-86).

Potential Indicators of Espionage, Terrorism, or Subversive Activity

Being a spy requires that one engage in certain observable behaviors. There is usually some personal contact with a foreign intelligence operative who recruits the spy or to whom the spy volunteers his or her services. The spy must obtain information, often information to which the spy does not have normal or regular access. This information usually needs to be copied and then removed from the office. The information is then communicated to the foreign intelligence service, and this often requires keeping or preparing materials at home and traveling to signal sites or secret meetings at unusual times and places. The spy may receive large sums of money which then may be deposited, spent, or hidden. Periods of high stress sometimes affect the spy's behavior.

Behaviors associated with espionage or terrorism sometimes deviate from the norm in such a way that they come to the attention of other people and must be explained. Other people sometimes become suspicious and pass their suspicions on to others. This sometimes comes out during a security clearance reinvestigation.

While an indicator's existence may be known, the counterintelligence implications of the indicator are frequently not recognized. Even in circumstances where the indicator has aroused suspicion, personnel may fail to act, or act improperly on that knowledge. The record of past espionage cases shows that coworkers and supervisors often ignored or failed to report counterintelligence indicators which, had they been reported, would have permitted earlier detection of the spy. In some cases, disciplinary actions were taken against the offender, but the matter was never considered from a counterintelligence perspective. See related information in the file [Reporting Espionage Indicators](#).

Indicators of Recruitment

- Close association with an individual who is known to be, or is suspected of being, associated with a foreign intelligence or security organization.

- Being secretive about contact with any foreign national or visit to a foreign diplomatic facility.
- Failure to report a personal relationship with any foreign national when reporting foreign contacts is required and expected.
- Failure to report an offer of financial assistance for self or family from a foreign national other than close family.
- Failure to report a request for classified or sensitive unclassified information by a foreign national or anyone else not authorized to receive it.
- Unreported private employment or consulting relationship on the side, separate from one's regular job, with a foreign national or foreign organization.
- Bragging about working for a foreign intelligence service or about selling U.S. technology. (Such statements should be taken seriously. They indicate at least that the individual is thinking about it, if not doing it.)

Indicators of Information Collection

- Accessing or attempting to access or download information to which the individual is not authorized access.
- Conducting key word searches in a classified database on people, places, or topics about which the individual has no need-to-know.
- Ordering classified or other protected documents or technical manuals not needed for official duties.
- Unusual pattern of computer usage (accessing files for which has no need-to-know) shortly prior to foreign travel.
- Asking others to obtain or facilitate access to classified or unclassified but sensitive information to which the individual does not have authorized access.
- Unusual inquisitiveness or questioning of coworkers about matters not within the scope of the individual's job or need-to-know.
- Obtaining or attempting to obtain a witness signature on a classified document destruction record when the witness did not observe the destruction.
- Copying protected information in other offices when copier equipment is available in the individual's own work area.
- Intentionally copying classified documents in a manner that covers or removes the classification markings.
- Extensive use of copy, facsimile, or computer equipment to reproduce classified, sensitive, or proprietary material which may exceed job requirements, especially if done when others are not present.

- Repeatedly working outside normal duty hours when this is not required and others are not in the office, or visiting classified work areas after normal hours for no logical reason.
- Repeated volunteering for assignments providing a different or higher access to classified or sensitive information.
- Bringing a camera, microphone, or recording device, without approval, into a classified area.
- Unauthorized monitoring of electronic communications.
- Illegal or unauthorized entry into any information technology system.
- Deliberately creating or allowing any unauthorized entry point or other system vulnerability in an information technology system.

Indicators of Information Transmittal

- Unauthorized removal or attempts to remove classified, export-controlled, proprietary or other protected material from the work area.
- Storing classified material at home or any other unauthorized place.
- Taking classified materials home or on trips, purportedly for work reasons, without proper authorization.
- Retention of classified, export-controlled, proprietary, or other sensitive information obtained at a previous employment without the authorization or the knowledge of that employer.
- Providing classified or sensitive but unclassified information, including proprietary information, outside official channels to any foreign national or anyone else without authorization or need-to-know.
- Regularly exchanging information with a foreigner, especially work-related information, whether or not the known information is sensitive.
- Putting classified information in one's desk or briefcase.
- Downloading classified material to an unclassified computer or storage device.
- Communicating electronically or using the Internet in a manner intended to conceal one's identity, e.g., use of "anonymizer" software on one's home computer or use of public computer services at a public library or Internet Café.
- Excessive and/or unexplained use of e-mail or fax.
- Short trips to foreign countries or within the United States to cities with foreign diplomatic facilities, for unusual or unexplained reasons, or that are inconsistent with one's apparent interests and financial means. This includes a pattern of weekend travel not associated with recreation or family.

- More than one trip during a two-year period to a country where one has no relatives, no business purpose for the travel, and where the country is not a common location for an annual vacation.
- Hesitancy or inability by traveler to describe the location reportedly visited.
- Any attempt to conceal foreign travel.
- Foreign travel with costs out of proportion to time spent at the foreign location.
- Frequent foreign travel with costs above the individual's means.
- Foreign travel not reflected in the individual's passport to countries where entries would normally be stamped.
- Maintaining ongoing personal contact, without prior approval, with diplomatic or other representatives from countries with which one has ethnic, religious, cultural or other emotional ties or obligations, or with employees of competing companies in those countries.
- Recurring communication with a person or persons in a foreign country that cannot be explained by known family, work, or other known ties.
- Illegal or suspicious acquisition, sale, or shipment of sensitive technology.
- Purchase of high quality international or ham radio-band equipment by other than a known hobbyist.

Indicators of Illegal Income

- Sudden, unusual ability to purchase high-value items such as real estate, stocks, vehicles, or foreign travel when the source of income for such purchases is unexplained or questionable.
- When asked about source of money, joking or bragging about working for a foreign intelligence service or having a mysterious source of income.
- Implausible attempts to explain wealth by vague references to some successful business venture, luck in gambling, or an unexplained inheritance; also more explicit explanations of extra income that do not check out when investigated.
- Living style and assets out of line with the individual's known income, especially if this has been preceded by signs of financial distress such as delinquencies or bankruptcy.
- Sudden decision to become a big spender; for example, picking up the bar bill for everyone, buying new and expensive clothes, giving expensive jewelry to a girl friend, all with vague explanation of the source of funds.

- Sudden reversal of a bad financial situation as shown by repayment of large debts or loans with no credible explanation of the source of funds.
- Extensive or regular gambling losses that do not appear to affect lifestyle or spending habits.
- Display of expensive purchases or large amount of cash shortly after return from leave, especially if the leave involved foreign travel.
- Foreign bank or brokerage account with substantial sums of money, but with no credible explanation for the source of this money or no logical need to maintain funds outside the United States.
- Large deposits to bank accounts when there is no logical source of income.
- Unexplained receipt of significant funds from outside the United States
- Moving funds into or out of the United States in amounts or circumstances that are inconsistent with normal business or personal needs. Includes deposit of large sums shortly after return from foreign travel.
- Large currency transactions as noted in Financial Crimes Enforcement Network (FinCEN) reports, unless the transaction was done for one's employer or a volunteer civic organization in which the individual is active.
- Carrying large amounts of cash when this is inconsistent with normal cash needs or known financial resources.

Indicators of Terrorist Activity

Although a terrorist might also steal information like a spy, the typical terrorist is engaged in planning, preparing, supporting or executing some violent terrorist action. The behaviors that might indicate or reveal terrorist preparations are quite different from the behavior of a spy. Alert employees who recognize and report these clues play a significant role in helping to protect our country against terrorist attacks and other subversive activities. The following are potential indicators that an individual may be involved in planning a terrorist attack.

- Talking knowingly about a future terrorist event, as though the person has inside information about what is going to happen.
- Statement of intent to commit or threatening to commit a terrorist act, whether serious or supposedly as a "joke," and regardless of whether or not it seems likely that the person intends to carry out the action. (All threats must be taken seriously.)
- Statements about having a bomb or biological or chemical weapon, about having or getting the materials to make such a device, or about learning how to make or use any such device—when this is unrelated to the person's job duties.

- Handling, storing, or tracking hazardous materials in a manner that deliberately puts these materials at risk.
- Collection of unclassified information that might be useful to someone planning a terrorist attack, e.g., pipeline locations, airport control procedures, building plans, etc. when this is unrelated to the person's job or other known interests..
- Physical surveillance (photography, videotaping, taking notes on patterns of activity at various times) of any site that is a potential target for terrorist attack (including but not limited to any building of symbolic importance to the government or economy, large public gathering, transportation center, bridge, power plant or line, communication center).
- Deliberate probing of security responses, such as deliberately causing a false alarm, faked accidental entry to an unauthorized area, or other suspicious activity designed to test security responses without prior authorization.
- Possessing or seeking items that may be useful for a terrorist but are inconsistent with the person's known hobbies or job requirements, such as explosives, uniforms (to pose as police officer, security guard, airline employee), high-powered weapons, books and literature on how to make explosive, biological, chemical, or nuclear devices.
- Possession of multiple or fraudulent identification documents.

Indicators of Support for Terrorism

As compared with espionage, which is usually conducted by individuals working alone, a terrorist attack is usually a group activity conducted by a small, clandestine cell which is often loosely associated with a larger network or organized group. Therefore, support for terrorism is often indicated by whom an individual associates with, certain public actions or Internet use, and or expressed support for a terrorist ideology.

Any support or advocacy of terrorism, or association or sympathy with persons or organizations that are promoting or threatening the use of force or violence, is a concern even if the individual is not directly involved in planning a terrorist attack. Of particular current concern is any expression of militant jihadist ideology, but this also includes the extremist groups discussed under [Allegiance to the United States](#).

- Knowing membership in, or attempt to conceal membership in, any group which: (1) advocates the use of force or violence to achieve political goals, (2) has been identified as a front group for foreign interests, or (3) advocates loyalty to a foreign interest over loyalty to the U.S. Government.

- Distribution of publications prepared by group or organization of the type described above.
- Pro-terrorist statements in e-mail or chat rooms, blogs, or elsewhere on the web. Frequent viewing of web sites that promote extremist or violent activity (unless this is part of one's job or academic study).
- Financial contribution to a charity or other foreign cause linked to support for a terrorist organization.
- Unexplained, or inadequately explained, travel to an area associated with terrorism or U.S. military action.
- Statements of support for the militant jihadist ideology of holy war against the West, such as: [6](#)

-- Militant jihad against the West is a religious duty before God and, therefore, necessary for the salvation of one's soul. Peaceful existence with the West is a dangerous illusion. Only two camps exist. There can be no middle ground in an apocalyptic showdown between Islam and the forces of evil.

-- The separation of church and state is a sin. Democratic laws are illegitimate and sinful, because they are "man-made" laws expressing the will of the electorate rather than God. The only true law is *Sharia*, the law sent down by God, which governs not only religious rituals but many aspects of day-to-day life.

-- Muslim governments that cooperate with the West and that have not imposed *Sharia* law are religiously unacceptable and must be violently overthrown.

- Statements of support for suicide bombers even though they kill innocent bystanders.
- Statements of support for violence against U.S. military forces either at home or deployed abroad.
- Statements of belief that the U.S. Government is engaged in a crusade against Islam.
- For U.S. military personnel only: Any action that advises, counsels, urges, or in any manner causes or attempts to cause insubordination, disloyalty, mutiny, or refusal of duty by any member of the armed forces of the United States. [7](#)

Other Behavioral Indicators

- Reporting by any knowledgeable source that the subject may be engaged in espionage or terrorist activities.
- Attempt to conceal any activity covered by one of the other counterintelligence indicators.

- Behavior indicating concern that one is being investigated or watched, such as actions to detect physical surveillance, searching for listening devices or cameras, and leaving "traps" to detect search of the individual's work area or home.
- Misrepresenting or failing to report use of an alias and/or multiple identities; possession of false identity documents without valid explanation.
- Attempts to place others under obligation through special treatment, favors, gifts, money, or other means.
- Avoiding or declining an assignment that would require a counterintelligence polygraph.
- Withdrawing application for a security clearance, or resigning from employment, in order to avoid a polygraph examination or other investigative interview.

Footnotes

1. This list is a combination and consolidation of many lists prepared by various persons and organizations for various purposes during the past 15 years.

2. Office of the National Counterintelligence Executive, Annual report to Congress on foreign economic collection and industrial espionage - 2005. NCIX 2005-10006, April 2005.

3. Krofcheck, J.L., & Gelles, M.G. (2006). Behavioral consultation in personnel security: Training and reference manual for personnel security professionals. (Appendix A: Assessing Competing Identities). Yarrow Associates.

4. Several government agencies have conducted comprehensive psychological assessments of their employees arrested for espionage, and an Intelligence Community project has interviewed and administered psychological tests to a number of Americans serving jail terms for espionage. Most interviews and tests were conducted after conviction and incarceration and were subject to agreements that protect the privacy of the offenders. Privacy and security considerations preclude public release of these studies.

5. Gottfredson, M.R., & Hirschi, T. (1990). A general theory of crime. Stanford, CA: Stanford University Press. Parker, J.P., & Wiskoff, M.F. (1992). Temperament constructs related to betrayal of trust (Tech. Report 92-002). Monterey, CA: Defense Personnel Security Research Center. Collins, J.M., & Schmidt, F.L. (1993). Personality, integrity, and white collar crime: A construct validity study. *Personnel Psychology*, 46, 295-311. Brodsky, S.L., & Smitherman, H.O. (1983). Handbook of scales for research in crime and

delinquency. New York: Plenum Press. Hogan, R., & Hogan, J. (1989). How to measure employee reliability, 74, 273-279. Collins, J.M., & Muchinsky, P.M. (1994). Fraud in the executive offices: Personality differentiation of white collar criminality among managers. Paper presented at 23rd International Congress of Applied Psychology, Madrid, Spain.

6. Department of State. (2005, April). Global jihad: Evolving and adapting. Retrieved March 3, 2006, from <http://state.gov/s/ct/rls/45306.htm>

7. Department of Defense. (2003, Dec. 1). DoD Directive 1325.6, Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces. Retrieved April 14, 2006, from <http://www.dtic.mil/whs/directives/corres/pdf2/d13256p.pdf>