Protecting Yourself

- Keep yourself out of compromising positions. Avoid illegal, improper, or inappropriate actions that would leave you vulnerable to manipulation or blackmail
- Consume alcohol in moderation, if all. Do not attempt to "keep up" with your hosts in social settings
- Obtain a country specific pre-travel briefing for the country or countries you plan to visit. Your local RED DART representatives can provide a classified or unclassified briefing that will detail specific threats prior to ravel. Travelers should be aware of possible threats not only at their final destination but also at intermediate stops
- Act as if your every action is being captures on video. Unlike the United States, most countries do not have e an expectation of privacy. This may include restaurants, airplanes, offices, public spaces, and even your hotel room

Your individual contribution to the security of your company, military branch, federal agency, and nation is vital.

Suspicious incidents should be reported immediately to your facility security officer, DSS industrial security representative, DSS counterintelligence special agent, and/or your local RED DART representative.

These individuals will assess your information and determine if a potential CI concern exists.

When In Doubt, Report It Out!

Report suspicious activity to your local security official.

About Us

REDDART is a collaborative effort to provide the full spectrum of counterintelligence and counterespionage services to cleared industry throughout the United States.

RED DART includes representatives from:

- Defense Security Service
- Air Force Office of Special Investigations
- Naval Criminal Investigative Service
- Federal Bureau of Investigation
- U.S. Army 902nd Military intelligence group
- U.S. Army Criminal Investigations Division
- National Aeronautics and Space Administration Counterintelligence
- Homeland Security Investigations
- Defense Criminal Investigative Service
- Coast Guard Investigative Services
- Coast Guard Counterintelligence
- Department of Energy
- Department of Commerce

RED DART

COUNTERINTELLIGENCE AWARENESS

Protecting Yourself,
Your Company & Your Country!

REDDART

COUNTERINTELLIGENCE AWARENESS: Protecting Yourself, Your Company & Your Country!

This brochure is intended to:

- Sensitize you to foreign intelligence entities targeting and elicitation
- Assist you in recognizing and countering recruitment attempts
- Encourage you to immediately report any suspicious incidents or encounters

The Threat

The mainstay of most intelligence services is the recruitment of well-placed assets who can provide insightful intelligence on collection requirements.

Most sensitive military and civilians jobs are of special interest to foreign intelligence entities.

Foreign intelligence entities use foreign defense industry representatives involved in business with U.S. companies to identify, assess, and approach potential recruitment targets.

>> **Despite the number of Americans who have initiated espionage careers on their own volition, foreign intelligence entities continue to invest a considerable time and resources in assessing and targeting U.S. citizens for recruitment.**

>> **Approaches are almost never made impulsively, but are actually the result of detailed planning and thorough assessment of the target. By the time the target is asked to work for the intelligence entity, the target is probably aware that a dubious relationship is developing.**

Elicitation

In the espionage trade, intelligence officers use elicitation as a technique to subtly extract information about, you, your work, and your colleagues. ***Elicitation is the art of conversation honed by intelligence entities to its finest edge.*** You never know if entities are using elicitation to pass the time or to gather intelligence.

Social networking offers almost unlimited opportunities to gather information through direct personal contact. Elicitation requires patience and persistence. Information collected over an extended period can provide the final piece tor the puzzle to a complex problem or save scarce research money.

Elicitation is non-threatening. It is hard to recognize as in intelligence gathering technique and is easy to deny any wrongdoing

Because elicitation is subtle and difficult to recognize, ***you should report any suspicious conversations as soon as feasible.***

Protecting Your Technological Information

Cleared contractors provide critical research and support to programs giving the United States an economic, technological, and military advantage. In a world where reliance on technology continues to grow, foreign entities have increased the targeting of electronic devices such as laptops, computers, and personal media such smart phones.

Travelers should report theft, unauthorized or attempted access, damage, and evidence of surreptitious entry of their portable devices.

The following countermeasures can decrease or prevent the loss of sensitive information:

- Leave unnecessary electronic devices at home
- Use designated travel laptop that only contains information required for your trip; limit proprietary or sensitive information
- Use temporary email address, not associated with your company
- Perform a comprehensive anti-virus scan on all electronic devices prior to departure and upon return
- Encrypt data, hard drives, and storage devices whenever possible
- Do not allow foreign electronic storage devices to be connected to your computer or cell phone
- Do not use thumb drives given to you — they may be compromised