COUNTERINTELLIGENCE

THE US NATIONAL STRATEGY

- Keep weapons of mass destruction, laser based weapons, advanced conventional weapons and related technology
- Protect the secrets of the U.S. Intelligence Community.
- Protect the nation's critical assets.
- Counter the activities of foreign spies.

COLLECTION METHODS

- Traditional direct and overt means
- Cyber exploitation
  - Spear Phishing
  - Watering Holes (compromised third party websites)
  - Removable media
- Attempted acquisition of and requests for information
- Academic solicitation
- Marketing and solicitation for marketing
- Foreign delegation visits

COUNTERMEASURES

Every region has active collectors. Axiologic Solutions employees must remain vigilant regardless of the collector's assumed country of origin. They will utilize all available means by which they can obtain the information they are seeking.

Your individual contribution to the security of our company, customers and nation is vital. Suspicious incidents must be reported immediately and directly to Security.

When In Doubt,… Report It Out!

AXIOLOGIC solutions

REPORTING REQUIREMENTS

CLEARED INDUSTRY'S ROLE

The technology and information resident in U.S. cleared industry is under constant and pervasive threat from foreign intelligence entities seeking to gain the technological edge. Increased awareness of the targeted information and methods of operation used by foreign entities is critical to improving our ability to identify and thwart collection attempts.

REPORTABLES

Axiologic Solutions employees must report efforts by an individual, regardless of nationality, to obtain illegal or unauthorized access to protected information or to compromise a cleared employee. Immediately report to Security all instances of:

- Mishandling of Classified Information
- Misuse of Information Systems
- Suspicious Cyber Incidents
- Foreign Influence
- Suspicious Contacts
- Suspicious Financial Activity
- Discovery of Recording Devices
- Adverse Information

Your timely and accurate reporting is the primary tool used to identify and mitigate collection efforts targeting our information and technology.

BE ALERT! BE AWARE!

For more information, contact 571-252-9461 Security.

AXIOLOGIC solutions

INSIDER THREAT

DEFINITION

Insider Threat: A person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or businesses through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities.

COMMON MOTIVATIONS

- Revenge
- Romance
- Ego
- Ideology
- Gullibility
- Money
- Coercion

BEHAVIORAL INDICATORS

- Dramatic changes in behavior or attitude
- Frequent, unreported, or unusual travel
- Financial delinquencies/affluence
- Disregard for security practices
- Unreported foreign influence or connections
- Crisis of conscience

SEE SOMETHING, SAY SOMETHING!

Axiologic Solutions Employees are responsible for reporting threats against national security. If you observe suspicious behavior, do not, under any circumstances, confront the individual(s). Instead, seek assistance from Security.

AXIOLOGIC solutions