Counterintelligence in the Private Sector

- San Diego ISAC Counterintelligence Sub-Committee – February 2016 -

WHY COUNTERINTELLIGENCE?
For starters, let's look at a few of the requirements as set in the National Industrial Security Program Operating Manual and existing Industrial Security Letters:

> NISPOM 1-300: states that a contractor "shall establish such internal procedures as are necessary to ensure that cleared employees are aware of their responsibilities for reporting pertinent information to the FSO, the FBI or other Federal authorities as required by this manual…"
>
> NISPOM 1-301: states that a contractor shall "promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable or possible espionage, sabotage, terrorism, or subversive activities at any of its locations. An initial report may be made by phone, but it must be followed in writing, regardless of the disposition made of the report by the FBI. A copy of the written report shall be provided to the CSA."

ISL 2006-02(4) – Suspicious contact reports will be submitted to the DSS Field Office.

ISL 2010-02 – Emphasizes the fact that cyber intrusions fall under NISPOM 1-301 as "actual, probable or possible espionage sabotage, terrorism or subversive activities" and as such, must be reported to local FBI and DSS offices.

Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. Many cleared defense contractors (CDC) are developing corporate counterintelligence programs to uncover and prevent foreign espionage campaigns targeting sensitive military data and technologies. Private sector counterintelligence (CI) offices are normally embedded in security departments and focus on protection against foreign intelligence collection and industrial espionage.

ISN'T THAT GOVERNMENT'S RESPONSIBILITY?

U.S. government oversight agencies rely on industry to remain vigilant and report any suspicious contacts to them. As CDC's, we must recognize potential collection attempts and report them to our government partners. The Defense Security Service (DSS) is chartered to oversee the protection of Department of Defense (DoD) technologies and contracts resident in the cleared industrial base. Corporate – Government partnership is critical to protecting information and technology. CDC's are required to report potential collection attempts by adversaries, be them state sponsored or otherwise, to DSS.

HOW DOES CI FUNCTION IN THE PRIVATE SECTOR?

An effective CI program enhances our ability to protect against economic espionage and theft of trade secrets that could negatively impact the economic stability and viability of a company. Training the workforce to recognize indicators of suspicious contacts is one way to better protect our information and employees. Educating employees what and how to report is an imperative component of the U.S. CI program.

Adversaries may target us in different domains to include conferences and trade shows, while overseas on foreign travel, or via cyberspace. CI offices conduct briefings and training presentations to enhance employees' awareness of who targets us, what they target, and the methodologies they employ to gain access to restricted information across these different domains.

An informed workforce enhances a company's ability to better protect their information, technologies, manufacturing processes, and competitive advantage. We can build fences and firewalls to keep bad guys out. A strong company CI program augments these defensive measures. Security conscious employees are better able to recognize actual or probable suspicious incidents and quickly report them, to include threats that may already be lurking inside our fences and firewalls.

WHAT HAPPENS WHEN A REPORT IS MADE?

A Facility Security Officer or an assigned member of the security staff is most often the contact point that compiles and forwards suspicious contact reports (or other matters of CI interest) to DSS. DSS receives the reports from all CDC's and conducts data aggregation and analysis of methodologies to gather as much information as possible to include: who instigated the attempt, where it came from, what it's aim was, and what methods of collection it used. DSS conducts a comprehensive analysis of information from across all companies and elements of cleared industry to form the basis of global CI threat trends, and feeds the information back to CDC's. This builds awareness, maintains visibility on emerging and evolving threats, and informs our defenses against them. In some instances DSS refers cases of CI concern to other federal law enforcement agencies such as the Federal Bureau of Investigation (FBI), or intelligence agencies for potential investigation, exploitation, or neutralization.

I DON'T HAVE A CLEARANCE OR HANDLE CLASSIFIED INFORMATION

Corporate trade secrets are in jeopardy. These are the same secrets that make companies profitable. "Trade secrets" are defined as all forms and types of financial, business, scientific, technical, economic or engineering information; which have an independent economic value as the result of being restricted to the public. It is commonly referred to as proprietary information, economic policy information, trade information, proprietary technology, or critical technology. Adversaries can be both state sponsored, and corporate competitors. Sensitive but unclassified proprietary information is extremely important to companies, and its loss, theft, or compromise can severely impact profits, competitiveness, and viability in a negative manner.

CONCLUSION

The private sector plays a critical role in preserving national security. Government agencies cannot do it alone. It is our collective responsibility to our country and companies to protect sensitive and classified information from unauthorized disclosure or compromise. The more we understand the threat, the better chance we have of thwarting our adversaries. Contact the CI working group for more information on how to increase your CI awareness or build a CI program at your company.