The Defense Security Service Counterintelligence Road Map For Industry

Professionals must understand the unique risks inherent to operating in a globally connected and competitive environment. A clear risk assessment will provide the tools to manage competitive pressures and employ counterintelligence strategies and techniques to most effectively counteract the threat.

Fundamentals of a Successful Counterintelligence (CI) Program

- Learn how the risk equation applies to your company/facility
- Instill a culture of risk awareness to ensure information is protected
- Build a culture of CI awareness and timely, accurate threat reporting
- Hire trained risk professionals with the authority to act
- Create security partnerships across the organization and management to share, promote, and achieve security success
- Work with DSS to ensure government and company shoulder risks appropriately, equitably, and together
- Confront cyber threats aggressively across all its venues
- Manage and report foreign travel and foreign visitors
- Establish an insider threat program with senior leadership support across counterintelligence, security, force protection, information assurance, and human resources

To manage threats, professionals must understand risk management and its elements: threat, vulnerability, consequence, and value.

Threat

The adversary's attempts to steal protected information and technology

Vulnerability

Gaps or weaknesses in the security barrier the adversary can exploit

Consequences

The damage to the U.S. government and company resulting from the adversary's theft

Value

The benefit to the adversary of acquiring the protected information and technology

Defense Security Service
27130 Telegraph Rd.
Quantico, VA 22134
www.dss.mil