COUNTERINTELLIGENCE VULNERABILITY ASSESSMENT FOR CORPORATE AMERICA

DEFINING COUNTERINTELLIGENCE (CI)

COUNTERINTELLIGENCE IS A PROACTIVE DISCIPLINE THAT DETERMINES WHETHER AGENTS OF A FOREIGN GOVERNMENT OR A FOREIGN COMPETITOR ARE USING COMPANY PERSONNEL OR OTHER MEANS TO STEAL INFORMATION OR TECHNOLOGY. ITS MISSION IS TO PROTECT A COMPANY'S CLASSIFIED AND PROPRIETARY TECHNOLOGIES FROM THEFT AND PROTECT ITS MOST VALUABLE ASSET—ITS PERSONNEL—FROM COMPROMISE.

To prevent foreign entities from achieving their goals, a Counterintelligence Program (CIP) proactively searches for and uses information from multiple sources. An effective CIP draws information from security programs and other internal systems, as well as from the U.S. Intelligence Community (USIC). Once this information is assembled, an effective CIP develops a coherent picture and crafts a strategy to prevent the foreign entity from successfully achieving its goals and minimizes the damage already done. An effective CIP conducts active analysis of available information, requires annual CI education for all employees, and provides a system for immediate referral of behavior with CI implications.

THE ESSENTIAL ELEMENTS OF A CI PROGRAM INCLUDES:

- **A central entity accountable for executing the program company-wide**
  - Reporting structure for all CI personnel
  - Liaisons with the USIC and/or US Government (USG) project sponsors
- **Recognition of the Insider Threat potential**
  - High value and unique access personnel are identified and briefed
  - A system exists to identify patterned behavior with possible CI implications
  - Liaisons with the FBI when possible espionage activity is identified
- **Recognition of the Foreign Threat potential**
  - Liaisons with the FBI/USG to discuss the foreign governments, organizations, and competitors who are targeting technologies and information owned/used by the company.
- **Integration of CI and Information Technology (IT)**
  - Trip wires exist to recognize anomalies with CI implications
  - CI and IT personnel work closely on network architecture and security, including cyber attacks, intrusions, and suspicious incidents.
- **Valuable Partnerships**
  - Internal and external liaisons with the USIC
- **Training**
  - CI training is required and tailored to specific programs and positions

EFFECTIVE CI PROGRAMS RECOGNIZE:

- The CI discipline and Security discipline are different and unique
- All personnel require CI awareness and certain employees require special awareness training
- A strong link between IT security and CI is essential in the global workplace
- The company can improve its protection through relationships with the USIC and USG

ELEMENTS OF SUCCESSFUL CI MANAGEMENT AND SUPPORT

A successful Counterintelligence Program (CIP) has a designated individual or Program Manager responsible for developing and implementing the program and is accountable for the program's success. Initially, the Program Manager may reside in the Security Office. The Program Manager should:

- Have a centralized command, control, and reporting system
- Participate in key information nodes and decision points within the company
- Proactively seek avenues to acquire information
- Identify circumstances that could put the company at risk

PROGRAM MANAGEMENT AND SUPPORT ELEMENTS		
ESSENTIAL PROGRAM ELEMENTS	Yes	No
1. The Program Manager is responsible for the development and implementation of the CIP.		
2. The CIP is centralized and all personnel with CI responsibilities report to the Program Manager.		
3. The Program Manager liaisons with the FBI/USG to discuss the foreign governments, organizations, and competitors who are targeting technologies and information owned/used by the company.		
4. Each sub-component/major program within the company has an individual responsible for CI matters; including ensuring program requirements are met.		
BENEFICIAL PROGRAM ELEMENTS		
5. The Program Manager participates in key company boards or councils, e.g., leadership councils, IT security councils, personnel disciplinary boards, business development teams (especially with regard to foreign business ventures), etc.		
6. The Program Manager provides standardized guidance and oversight for persons in all sub-components/major programs.		
7. The Program Manager has received professional training in counterintelligence.		
8. Employee records are centralized and accessible to the Program Manager.		
RECOMMENDED PROGRAM ELEMENTS		
9. Designated persons in all sub-components/major programs have received professional training in counterintelligence.		
10. The CIP has sufficient support—staff, funding, analytical capability, access to relevant reports, etc.—commensurate with the company's size, research, client base, and the sensitivity of its programs and activities.		

ELEMENTS OF THE INSIDER THREAT

Despite multiple layers of protection "insiders" have proven to be the most effective penetration tool for foreign governments and intelligence services. Insiders betray their company for a number of reasons, including money, revenge or ideology. While all employees are potentially an insider threat, not all warrant the same level of CI precautions. All employees should have a basic CI awareness, but beyond that an effective program identifies personnel who are of high value to the company or possess unique access within the company for additional CI awareness training. The baseline question for determining who is of high value or who has unique access is –what is the significance of the damage that will occur if this person were recruited by a foreign government or competitor?

High value and unique access personnel:

- Are critical to project success
- Are associated with critical programs
- Have access to critical internal systems or technologies
- If compromised, could significantly impact National Security (intelligence or military programs) or the company's economic viability

A system to identify and document suspicious activity by persons who:

- Inquire above their security clearance
- Access sensitive information during odd hours
- Query and/or collect unusually large amounts of information
- Ask questions about projects they are not involved with
- Are patterned in their suspicious behavior

Categories of conduct that may be exploitable for the purpose of coercion may include:

- The loss of security clearance
- Financial anomalies
- Disciplinary action and dismissals
- Unreported contacts with foreign nationals
- Unauthorized access to secure systems
- Marked changes in behavior

A comprehensive and centralized personnel information system should include:

- Data on clearance level
- Foreign travel
- Regular business contact with foreign nationals
- Disciplinary actions
- Arrests or police incident records
- Exploitable conduct allegations
- Security infractions or withdrawal of a clearance
- Other information that contributes to a comprehensive picture of the employee.

ELEMENTS OF THE INSIDER THREAT		
ESSENTIAL PERFORMANCE ELEMENTS	Yes	No
1. Executive Management recognizes that the "Insider Threat" is real and that company secrets/proprietary information could be stolen by their own employees.		
2. The company has a system to identify high-value and unique access personnel.		
3. The company has a system to identify and document individuals engaged in suspicious activity.		
4. The Program Manager is involved in the company's personnel proceedings, providing advice and CI input in the disciplinary process.		
5. The Program Manager liaisons with the FBI to report suspicions of possible espionage activity.		
6. The company has a process of documentation control to include marking and printing of proprietary documents, restricted access to proprietary documents, tracking of proprietary documents and control procedures		
7. The company has a system to manage after hours access through written policy, employee written acknowledgement, method of access, access logs maintained, and restriction of sensitive areas and method of restriction.		
8. The company has established legal security measures and maintains copies of all documents signed by employees to include non-disclosure agreements, non-competition agreements, assignment of inventions, acknowledgement that the employee has read and understood the company policies on proprietary information and a signed statement that the employee has not brought trade secrets or proprietary information from any former employer.		
BENEFICIAL PERFORMANCE ELEMENTS		
9. The Program Manager is knowledgeable of the company's highly sensitive programs and projects, such as Special Access Programs (SAPs), and WMD technology that would be likely targets for an insider threat.		
10. The Program Manager has defined categories of conduct that may be exploitable for the purpose of coercion.		
RECOMMENDED PERFORMANCE ELEMENTS		
11. The company requires all personnel to report foreign travel, hosting of foreign nationals, or contact with foreign nationals, especially those from high threat countries to the Program Manager.		
12. The company has a comprehensive and centralized personnel information system.		
13. The company has a policy regarding employees departing the company, conducts exit interview and obtains signed acknowledgement from employee documenting they do not possess proprietary information.		

ELEMENTS OF THE FOREIGN THREAT

To protect itself, the company must know which countries are targeting which technologies. Classified and export restricted technology is identified by the USG, but the company should also identify the proprietary and unclassified information that may be of interest to outsiders. A credible, dynamic perception of the threat is key to the company's viability and economic future. A successful CIP has a clear understanding of visitors, new hires, subcontractors, vendors, travelers, employees assigned overseas, and high value and unique access employees. In addition, the company partners with internal and external entities to ensure the success of the CIP. Lastly, the company provides the appropriate level of CI awareness training to its personnel.

ELEMENTS OF THE FOREIGN THREAT		
ESSENTIAL PERFORMANCE ELEMENTS	Yes	No
1. Executive Management recognizes the threat posed by foreign intelligence services and economic competitors.		
2. The company has a system to identify proprietary information that could be targeted by foreign intelligence services and economic competitors which includes documentation with a description of the proprietary information and why it is proprietary.		
3. The company has clearly defined requirements for protecting proprietary information as well as identified classified and export restricted technology.		
4. The company has a system to identify engineers, HR personnel, legal personnel, technical employees or others who will be in a position to review and testify about stolen or compromised proprietary information		
5. The company has enacted physical security measures to include security guards, identification badges, visitor sign-in/badges/escort procedures, maintenance of visitor logs.		
6. Personnel who host foreign visitors are directly responsible for ensuring that company imposed conditions and restrictions placed on visitors are maintained and that they closely monitor the contacts and activities of all visitors.		
7. The Program Manager liaisons with the FBI to report visits by non-US persons and any suspicion of possible espionage activity.		
BENEFICIAL PERFORMANCE ELEMENTS		
8. The company conducts analysis of information regarding foreign visitors to classified/high risk programs.		
9. The company documents and analyzes the foreign travel history of employees and other suspicious patterns of behavior such as recurring theft/ loss of laptops, thumb drives, etc.		
RECOMMENDED PERFORMANCE ELEMENTS	Yes	No
10. The company requires all personnel to attend foreign travel briefings.		
11. Employees are encouraged to report unsolicited emails and foreign contacts.		

ELEMENTS OF CI-INFORMATION TECHNOLOGY SECURITY

A successful CIP addresses the cyber-borne threat to a company's information, technologies, and personnel. The company uses information technology (IT) tools to augment the CI program, especially in addressing the insider threat.

The virtual cyber world significantly expands access to sensitive information for the public at large, foreign intelligence services, foreign competitors, and the "insider." As a result, the partnership between IT security and CI is crucial to fully protect sensitive information while providing access to those who need it. This protection/access balance is significantly strengthened by a CI trained cyber security cadre who interact with the CI Program Manager and other CI personnel in a mutually beneficial way. This begins with an understanding of the difference between traditional IT security (secure passwords, security plans, vulnerability scanning, etc.) and cyber security with a CI focus (intrusion detection systems placed on sensitive and classified networks, vulnerability scanning for repeated high vulnerabilities in certain machines or those associated with certain high value individuals).

Beneficial IT information includes:

- Intrusion attempts
- Unsolicited email from threat countries
- Hits on web sites
- Anomalous activity on the internal network

The CIP can collate the IT information with other available information including:

- Visitors from threat countries
- Foreign travel
- Employees with access to sensitive information
- Knowledge of entities targeting the company's information

ELEMENTS CI-IT SECURITY		
ESSENTIAL PERFORMANCE ELEMENTS	Yes	No
1. IT security personnel know how foreign intelligence services and economic competitors attack IT systems.		
2. The company has electronic security measures in place to include the following: - Identify operating systems used - Computer links to Internet - Use of firewalls and frequency of updating - Employee restriction to proprietary information, audit system - Use of passwords/frequency of change - Generation and maintenance of network logs - Employee use of laptops - Laptop features (mass storage media and storage requirements) - Email restrictions - Email activation process for new hires (when) - Email deactivation for departing employees (when) - Restrictions on non-company software/auditing procedures - Frequency of backups on work/home computers - Backups: type of media used/archival procedures		
2. Protective mechanisms/trip wires are in place for recognizing anomalies that could have CI implications.		
3. Systems and network administrators with access to sensitive and classified networks are recognized as high-value employees and have appropriate clearances.		
4. Vulnerability scanning is conducted regularly and a process ensures that security patches are promptly and correctly installed.		
5. The company reviews all laptops, thumb drives, cell phones, and PDAs taken out of the U.S. to determine if they have been compromised. Electronic media utilized outside the company's IT system is checked for integrity prior to introduction.		
6. Cyber attacks, intrusions, suspicious incidents, and other anomalies discovered by IT security personnel are reported to the CI Program Manager.		
BENEFICIAL PERFORMANCE ELEMENTS		
7. IT security personnel, network and systems administrators, and the CI Program Manager interact using such forums as incident response teams, network architecture and IT security planning groups, and others to prepare for and respond to cyber incidents.		
8. System and network administrators are given tailored CI awareness training.		
9. Foreign national access to sensitive IT resources is carefully monitored and controlled.		

RECOMMENDED PERFORMANCE ELEMENTS	Yes	No
10. Remote access to company IT resources is limited and carefully monitored.		
11. A CI risk assessment is conducted prior to granting remote access.		
12. The company website is free of sensitive information, including personnel information.		
13. Company personnel travel with a "clean" laptop containing only information necessary for purpose of the travel, laptops and electronic media/devices are scanned upon return for compromise.		
14. High value information necessary for business continuity only resides on IT systems with no physical connectivity to the Internet.		

ELEMENTS OF EFFECTIVE PARTNERSHIPS

Successful CI programs depend on effective internal and external partnerships. Internal partnerships not only includes personnel with security and counterintelligence responsibilities, but also personnel responsible for ITAR compliance, information assurance, human resources, foreign travel and deployments, training, and the purchasing of services and products. External partnerships are those liaisons with members of the USIC, especially the FBI, DoD, and CIA. For maximum effectiveness, these partnerships are embedded within the company at key decision points.

ELEMENTS OF INTERNAL AND EXTERNAL PARTNERSHIPS		
ESSENTIAL PERFORMANCE ELEMENTS	Yes	No
1. The CI Program Manager engages in effective working relationships with the USIC.		
2. There is a centralized CI information sharing system within the company's formal security apparatus.		
BENEFICIAL PERFORMANCE ELEMENTS		
3. The CI Program Manager participates in the company's internal council or working groups that address human resource, cyber security, business development, and other groups that address issues or problems that might have counterintelligence and security implications.		
4. Liaisons with the FBI and USIC to identify countries known to aggressively collect information on classified programs, high-end R&D, or export restricted technology, or other intellectual property.		
5. Liaisons with the FBI and the USIC to identify current trends in collection activities of foreign intelligence services and others.		
RECOMMENDED PERFORMANCE ELEMENTS		
6. The CI Program Manager explores CI partnerships with counterparts in industry to keep abreast of CI-relevant issues, problems, and threats unique to the corporate environment.		

ELEMENTS OF EFFECTIVE CI TRAINING

An effective CIP begins with a CI educated workforce. All employees, not just employees holding U.S. Government security clearances, should have CI awareness training. Certain populations within the workforce should receive additional training based on their access to classified information, proprietary information and high value unclassified information; based on their assignments, their travel, and their foreign interactions. Certain positions, such as computer network administrators, should receive training to spot cyber activities which may have CI implications.

- Annual CI briefing for cleared and non-cleared personnel
    - Recognizing and reporting suspicious behavior
    - Reporting requests for information from unsolicited contacts, including email
- High value employee training
    - Increase awareness of the threat posed to them and to the company by foreign intelligence services and foreign competitors
    - Increase awareness of how sensitive and working papers in addition to classified and proprietary programs are targets for collection
- Foreign travel briefs
    - Provided for both official and unofficial travel
    - Explain common targeting methods, how to recognize when you are being targeted, and how to respond

ELEMENTS OF EFFECTIVE TRAINING		
ESSENTIAL PERFORMANCE ELEMENTS	Yes	No
1. The company has a required, annual CI awareness training for both cleared and non-cleared personnel.		
2. CI awareness training for all high value employees is required and tailored to specific programs and the nature of the position.		
3. Company employees who travel outside the US and employees on foreign assignments are given a brief on foreign intelligence service targeting prior to departure and are debriefed upon their return.		
4. Company policy requires that employees report suspicious incidents and unsolicited contacts by foreign nationals and others.		
BENEFICIAL PERFORMANCE ELEMENTS		
3. The Company has a clear channel of communication for reporting suspicious activity, contacts, or other CI related concerns.		
RECOMMENDED PERFORMANCE ELEMENTS		
4. Sub contract employees on classified or sensitive projects receive CI awareness briefings.		