The purpose of this brochure is to provide information to security professionals, counterintelligence personnel, and cleared contractors which will aid them in recognizing suspicious contacts, and implementing threat appropriate, cost effective, and rational security countermeasures.

A summary of the suspicious contacts in 1999, reported by cleared defense contractors, indicates foreign entities employed a variety of Modus Operandi (MO) in attempting to acquire information. The following reported MOs along with the percentage employed in 1999 are as follows:

- **REQUESTS FOR INFORMATION- 45%**
- **FOREIGN VISITS- 14%**
- **SOLICITATION AND MARKETING OF SERVICES-11%**
- **ACQUISITION OF TECHNOLOGY & COMPANIES-9%**
- **EXPLOITATION OF INTERNET (HACKING)- 6%**
- **EXPLOITING JOINT VENTURES AND JOINT RESEARCH- 5%**
- **TARGETING AT INTERNATIONAL CONVENTIONS/EXHIBITS- 5 %**
- **FOREIGN EMPLOYEES- 2%**
- **TARGETING CULTURAL COMMONALITIES- 2**
- **TARGETING FORMER EMPLOYEES- 1%**

DSS has identified activities or circumstances that are part of these MOs, which can serve as indicators. While these indicators do not always equate to an actual foreign collection threat, they can serve as a signal. A number of indicators in a given situation might warrant further examination.

REQUESTS FOR INFORMATION.
Requests for US defense industry S&T program information are the most frequently reported MO associated with foreign collection activity. Requests frequently involve faxing, mailing, E-mailing, or phoning to individual US persons rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently being sent over the Internet. Marketing surveys, which were incorporated into requests for information, can elicit sensitive technological and business information. With this particular method it is important to consider who is the end user of the information and who is completing the survey. The Internet provides an excellent method of direct communication with government and US industry for foreign collection purposes. Internet access to a company's bulletin board, home page, and employees provide a foreign collector many avenues to broaden collection efforts.

Indicators

- The INTERNET address is in a foreign country.
- The recipient has never met the sender.
- Requester may be associated with an embargoed country.
- Technology requested is classified, International Traffic in Arms Regulation (ITAR) controlled, is on the Militarily Critical Technologies List (MCTL), or has both commercial and military applications.
- The requester identifies his/her status as a student or consultant.
- The requester identifies his/her employer as a foreign government or the work is being done for a foreign government or program.
- The requester asks about a technology related to a defense-related program, project, or contract.
- The requester asks questions about defense-related programs using acronyms specific to the program.
- The requester insinuates that the third party he/she works for is "classified."
- The requester admits he/she could not get the information elsewhere because it was classified or controlled.
- The requester advises the recipient to disregard the request if it causes a security problem or if it is for information the recipient cannot provide due to security classification, export controls, and so forth.
- The requester advises the recipient not to worry about security concerns.
- The requester assures the recipient that export licenses are not required or are not a problem.
- Marketing surveys may be faxed or mailed to an individual vice the company marketing office.
- Marketing surveys may be sent by foreign consortiums or a consulting company. Foreign companies with foreign intelligence involvement are likely to be a consortium of officials, military officers, or private interests.
- Marketing surveys often may exceed generally accepted terms of marketing information.
- Strong suspicions that the "surveyor" is employed by a competing foreign company.
- Surveys may solicit proprietary information concerning corporate affiliations, market projections, pricing policies, program or technology director's names, company personnel working on the program, purchasing practices, and types and dollar amounts of US Government contracts.
- Customer and supplier bases for a company may also be sent marketing surveys that exceed accepted terms of marketing information.

Recommended Security Countermeasures

- Have a written company policy on how to respond to requests.
- Brief employees not to respond to suspicious requests.
- Brief employees to report suspicious incidents to the Facility Security Officer (FSO).
- Review how much information you have in the open domain, i.e. do you have a WEB site and if so what's on it?
- Have a Technology Control Plan.
- Train employees to recognize and report suspicious marketing surveys.

INAPPROPRIATE CONDUCT DURING VISITS. Foreign visits to cleared US defense contractors can present potential security risks if sound risk management is not practiced.

Indicators

- Visitors are escorted by a Foreign Liaison Officer or embassy official who attempts to conceal their official identities during a supposedly commercial visit.
- Hidden agendas as opposed to the stated purpose of the visit, i.e. visitors arrive to discuss program X but do everything to discuss and meet with personnel who work with program Y.
- Last minute and unannounced persons added to the visiting party.
- "Wandering" visitors who act offended when confronted.
- Using alternative mechanisms. For example if a classified visit request is disapproved, the foreign entity may attempt a commercial visit.
- Visitors ask questions during briefing outside the scope of the approved visit hoping to get a courteous or spontaneous response.

Recommended Security Countermeasures

- Brief threat to all employees involved with the foreign visit.
- Ensure appropriate personnel , both escorts and those meeting with visitors, are briefed on the scope of the visit.
- The number of escorts per visitor group should be adequate to properly control movement and conduct of visitors.
- Have a Technology Control Plan.

SUSPICIOUS WORK OFFERS. Foreign scientists and engineers will offer their services to research facilities, academic institutions, and even cleared defense contractors. This may be a MO to place a foreign national inside the facility to collect on a desired technology.

Indicators

- Foreign applicant has a scientific background in a specialty for which his country has been identified as having a collection requirement for that technology.
- Foreign applicant offers services for "free." Foreign government or corporation associated with government is paying expenses.
- Foreign interns (students working on masters or doctorate) offer to work under a knowledgeable individual for free, usually for a period of 2-3 years.
- The technology in which the foreign individual wants to conduct research is frequently related to, or may be classified, ITAR , MCTL or export controlled.

Recommended Security Countermeasures

- Have a Technology Control Plan.
- Provide employees periodic security awareness briefings with regard to long-term foreign visitors.
- Check backgrounds and references.
- Request a threat assessment from the program office.

INTERNATIONAL EXHIBITS, CONVENTIONS, AND SEMINARS. These functions directly link programs and technologies with knowledgeable personnel.

Indicators

- Topics at seminars and conventions deal with classified or controlled technologies and /or applications.
- Country or organization sponsoring seminar or conference has tried unsuccessfully to visit the facility.
- Receive invitation to brief or lecture in foreign country with expenses paid.
- Requests for presentation summary 6-12 months prior to seminar.
- Photography and filming appears suspicious.
- Attendees wear false name tags.

Recommended Security Countermeasures

- Consider what information is being exposed, where, when, and to whom.
- Provide employees with detailed travel briefings concerning the threat, precautions to take, and how to react to elicitation.
- Take mock-up displays instead of real equipment.
- Request a threat assessment from program office.
- Restrict information provided to that necessary for travel and hotel accommodations.
- Carefully consider whether equipment or software can be adequately protected.

JOINT VENTURES/JOINT RESEARCH. Co-production and various exchange agreements potentially offer significant collection opportunities for foreign interests to target restricted technology.

Indicators

- Resident foreign representative faxes documents to an embassy or another country in a foreign language.
- Foreign representative wants to access the local area network (LAN).
- Foreign representative wants unrestricted access to the facility.
- Enticing US contractors to provide large amounts of technical data as part of the **bidding process**, only to have the contract canceled.
- Potential technology sharing agreements during the joint venture are one-sided.
- The foreign organization sends more foreign representatives than is necessary for the project.
- The foreign representatives single out company personnel to elicit information outside the scope of the project.

Recommended Security Countermeasures

- Review all documents being faxed or mailed and have someone to translate.
- Provide foreign representatives with stand alone computers.
- Share the minimum amount of information appropriate to the scope of the joint venture/research.
- Extensively educate employees on the scope of the project and how to deal with and report elicitation. Initial education must be followed by periodic sustainment training.
- Refuse to accept unnecessary foreign representatives into the facility.

FOREIGN ACQUISITION OF TECHNOLOGY AND COMPANIES. Foreign entities attempt to gain access to sensitive technologies by purchasing US companies and technology.

Indicators

- Companies of political and military allies are most likely associated with this activity.
- New employees hired from the foreign parent company or its foreign partners who wish to immediately access classified data.
- Foreign parent company may attempt to circumvent or mitigate the FOCI process.

Recommended Security Countermeasures

- Request a threat assessment from the program office.
- Scrutinize employees hired at the behest of foreign entity.
- Conduct frequent checks of foreign visits to determine if foreign interests are attempting to circumvent the security agreements.
- Provide periodic threat briefings to outside directors and user agencies.

CO-OPTING FORMER EMPLOYEES. Former employees who had access to sensitive, proprietary, or classified S&T program information remain a potential counterintelligence concern. Targeting cultural commonalities to establish rapport is often associated with the collection attempt. Former employees may be viewed as excellent prospects for collection operations and considered less likely to feel obligated to comply with US Government or corporate security requirements.

Indicators

- Former employee took a job with a foreign company working on the same technology.
- Former employee maintains contact with former company and employees.
- The employee alternates working with US companies and foreign companies every few years.

Recommended Security Countermeasures

- Brief employees to be alert to actions of former employees returning to the facility.
- Have a policy concerning visitation or contacts with current employees by former employees.
- Debrief former employees upon termination of employment and reinforce their responsibilities concerning their legal responsibilities to protect classified, proprietary, and export controlled information.

TARGETING CULTURAL COMMONALITIES. Foreign entities exploit the cultural background of company personnel in order to elicit information.

Indicators

- Employees receive unsolicited greetings or other correspondence from embassy of country of family origin.
- Employees receive invitations to visit country of family origin for purpose of providing lecture or receiving an award.
- Foreign visitors single out company personnel of same cultural background to work or socialize with.

Recommended Security Countermeasures

- Brief all employees on this MO and have a policy concerning the reporting of same.
- Monitor the activities of foreign visitors for indications of their targeting of company personnel.

If you believe that any of the above situations apply to your company, you should immediately notify your DSS Industrial Security Representative through your company Facility Security Officer. Likewise, notify DSS of any indication that your company or any of your employees may be the target of an attempted exploitation by the intelligence service or commercial interests of another country. **Reports of actual, probable, or possible espionage should be submitted to the FBI with a copy to DSS in accordance with the NISPOM.**

This brochure was prepared by the Counterintelligence Office of the Defense Investigative Service. If you would like to recommend additional security countermeasures, please contact your DSS Industrial Security Representative.

This brochure is approved for public release.
OASD-PA/97-S-1431.

Suspicious Indicators
And
Security Countermeasures
For
Foreign Collection Activities
Directed Against The
US Defense
Industry

FEBRUARY 2000