Suspicious Indicators and Security Countermeasures for Foreign Collection Activities Directed Against the United States

February 20, 2004

DEPARTMENT OF COMMERCE
Office of Security
Anti-Terrorism Division
Phone: (202)-482-2942
Fax: (202)-482-1098

TABLE OF CONTENTS

FOREIGN REQUESTS FOR INFORMATION

Foreign requests for U.S. industry Science and Technology (S&T) program information and technology are the most frequently reported method of operation (MO) associated with foreign targeting activity. Requests frequently involve faxing, mailing, e-mailing, or telephoning to individual U.S. persons rather than corporate marketing departments. The requests may involve surveys or questionnaires and are frequently sent over the Internet.

Indicators

The requester:

has an e-mail address is in a foreign country.
may be associated with an embargoed country.
identifies their status as a student or consultant.
identifies themselves as a “student” seeking empathy because his nation lacks this scientific or technical information
identifies their employer as a foreign government or the work is being done for a foreign government or program.
asks about a technology related to a defense-related program, project, or contract.
asks questions about defense-related programs using acronyms specific to the program.

insinuates that the identity of the third party they work for is “classified.”
admits they could not get the information elsewhere because it was classified or “controlled.”
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.
assures the recipient that export licenses are not required or are not a problem.
recipient has never met or does not normally conduct business with the sender.
is requesting technology that is classified, International Traffic in Arms Regulation (ITAR)-controlled, is on the Militarily Critical Technologies List (MCTL), or has both commercial and military applications.
requests may be faxed or mailed to an individual vice the company marketing office.
requests may exceed generally accepted terms of information.
gives strong suspicions that a competing foreign company employs the “surveyor.”

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
have a written policy on how to respond to requests.
brief employees not to respond to suspicious requests.
brief employees to report suspicious incidents to their security office or security focal point.
review how much information you have in the open domain.
ask foreigner why they want the information, who they represent, and what the U.S. information will be used for.

WEB-BASED REQUESTS FOR INFORMATION

Web-based requests continue to be a significant source of foreign targeting of U.S. information or technologies. A wealth of once protected information is now retrievable by individuals from around the world. There appears to be a sharp increase in the use of web-based requests by foreign entities as a means to identify potential targets and to facilitate the actual collection of information. Web-based requests provide a simple, low cost, non-threatening, risk-free means of worldwide attempts to acquire U.S. controlled information and technology. Web-based requests are inconspicuous and can bypass many traditional security safeguards, thus directly reaching the target.

Indicators

the program, project or company does not normally conduct business with the foreign requestor.
the request originates from an embargoed country.
the request is, in fact, unsolicited or unwarranted.
requestor claims to represent an official government agency but avoids proper channels to make the request.
the initial request is directed at an employee who does not know the sender and is not in the sales or marketing office.
the requestor is fishing for information.
requestor represents unidentified third party.
the requestor is located in a country with a targeting history directed at the United States.
the requestor appears to be “skirting controls.”
several similar requests are made over time.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
incorporate security in to web design and advertising.
initiate an active monitoring solution of web site.
report request to your Security Office.

SOLICITATION AND MARKETING OF SERVICES

Consistent with past reporting, individuals, companies and research facilities offer their technical and business services to U.S. research facilities, academic institutions and the cleared defense industry.

Indicators

foreign “scientist” seeks employment associated with sensitive defense technologies.
offer to provide offshore software support.
foreign government- and business- sponsored internships.
invitation to cultural exchange, individual-to-individual exchange or ambassador program.
offer to act as sales or purchasing agent in foreign country.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
report names of foreign scientists and engineers whose solicitation concerns classified or controlled research and technology.
obtain recommendations and assess risks posed by software support in a foreign land.
receive State Department travel briefings before departing on an exchange or ambassador program.

FOREIGN ACQUISITION OF U.S. TECHNOLOGY/COMPANY

Foreign entities try to access sensitive technologies by purchasing U.S. technology or a U.S. company possessing the sensitive technology/product.

Indicators

companies of political and military allies are most likely associated with this activity.
foreign competitors seek a position in the U.S. company that affords access to technology
new employees hired from the foreign parent company or its foreign partners ask to access classified data.
foreign parent company attempts to circumvent the security agreement or, even easier, avoids or otherwise disrupts or hinders the Foreign Ownership, Control or Influence (FOCI) process.
foreign parent employees try to make exceptions to the terms of the security agreement.
statement that license is not necessary.
foreign company asks U.S. company to send information or product to another U.S.-based company for transfer overseas or via Fedex or UPS to overseas address.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
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 security agreements.
provide periodic threat briefings to outside directors and user agencies.
ask what U.S.-based company does.
ask why the company cooperates with the foreign entity.
ask why the foreigner wants the product express-mailed.
ask export officer if information or technology is export-controlled.

FOREIGN VISITS AT U.S. FACILITIES

Foreign visits to U.S. facilities can present potential security risks if sound risk management is not practiced.

Indicators

a Foreign Liaison Officer or embassy official escorting visitor attempts to conceal official identities during a supposedly commercial visit.
hidden agendas as opposed to the stated purpose of the visit.
last minute and unannounced persons added to the visiting party.
“wandering” visitors who act offended when confronted.
using alternative methods. 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.
visitor claims business interest but lacks experience researching and developing this technology.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
brief country threat to all employees involved with the foreign visit. Request intelligence country threat assessments.
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.

EXHIBITS, CONVENTIONS AND SEMINARS

These functions directly link programs and technologies with knowledgeable personnel. Conventions may provide foreign entities with targeting information to be used later.

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 a foreign country with all expenses paid.
requests for presentation summary 6-12 months before seminar.
photography and filming appear suspicious.
attendees wear false name tags.
casual conversation and discussions during and after these events.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
be aware of follow-up requests after a show.
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/hotel accommodations.
carefully consider whether equipment or software can be adequately protected.

EXPLOITATION OF INTERNET

Internet exploitation consists of hacking, probes, scanning, and pinging. This category is not related to the Internet based requests for information. The majority of cases involve probing efforts. Although probing a system is legal, once a port is breached a crime is committed.

Indicators

computer probes are most likely searching for potential weaknesses in systems for exploitation.
network attacks originated from foreign Internet service providers .
attacks last over a period of a day.
several hundred attempts are made to use multiple passwords.

Recommended Security Countermeasures

have a Technology Control Plan (TCP) .
have firewall monitoring software that logs all intrusion attempts and any malicious activity.
have the appropriate level of protection in place to repel such an attack.
when a probe is noted, heighten security alert status.

JOINT VENTURE/ RESEARCH

Co-production and various exchange agreements potentially offer significant opportunities for foreign interests to target restricted technology.

Indicators

resident foreign representative:
faxes documents to an embassy or another country in a foreign language.
wants to access the local area network (LAN).
wants unrestricted access to the facility.
singles out company personnel to elicit information outside the scope of the project.
enticing U.S. 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.
foreign organization sends more foreign representatives than is necessary for the project.

Recommended Security Countermeasures

have a Technology Control Plan (TCP).
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. Periodic sustainment training must follow initial education.
refuse to accept unnecessary foreign representatives into the facility .

TARGETING OF U.S. PERSONNEL ABROAD

Suspicious activity occurs on collector's home territory leaving U.S. travelers vulnerable to exploitation, including that by Foreign Intelligence Services (FIS). Frequently, FIS recognize U.S. travelers who are engaged in international conventions, support to combined military operations, and joint ventures.

Indicators

technical means (for example, electronic surveillance).
entrapment schemes such as honey trap, black market and extortion.
repeated stays in the same room of the same hotel.
several attempts made to access room by service personnel.
excessively helpful assistance.
undue questioning by port authorities.

Recommended Security Countermeasures

have a Technology Control Plan (TCP) .
facilities should review the type and amount of information they provide.
withhold non-essential biographic and other data requested by the host.

WORK OFFERS

Foreign scientists, students, 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 information concerning a desired technology.

Indicators

foreign applicant has a scientific or engineering background in a technical area for which his country has been identified as having a collection requirement.
foreign applicant offers services for "free," stating that a foreign government agency, military activity, university, or corporation is paying expenses.
foreign intern (students working on masters or doctorate) offers to work without pay under a knowledgeable individual, usually for a period of 2-3 years.
the technology in which the foreign individual wants to work or conduct research is frequently related to, or may be classified, ITAR , EAR, CCL, MCTL controlled.

Recommended Security Countermeasures

have a Technology Control Plan (TCP) .
provide employees periodic security awareness briefings about long-term foreign visitors.
check backgrounds and references of foreign job, research, and intern applicants.
request a threat assessment from the program office whose program is associated with the foreign interest.

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 commonalties 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 U.S. Government or corporate security requirements.

Indicators

former employee takes a job with a foreign company working on the same technology.
former employee maintains contact with former company and employees .
an employee alternates working with U.S. companies and foreign companies every few years.

Recommended Security Countermeasures

have a Technology Control Plan (TCP) .
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 employees upon termination of employment and reinforce their responsibilities
concerning their legal responsibilities to protect classified, proprietary, and export controlled
Sensitive But Unclassified (SBU) information and technology .

TARGETING CULTURAL COMMONALITIES

Foreign entities exploit the cultural background of company personnel, visitors and visited, to elicit information.

Indicators

employees receive unsolicited greetings or other correspondence from embassy, company, or country of family's origin.
employees receive invitations to visit country of family's origin for purpose of providing lecture or receiving an award.
foreign visitors single out company personnel of same cultural background with whom to work or socialize.

Recommended Security Countermeasures

have a Technology Control Plan (TCP) .
brief all employees on this MO and address it in company reporting policy.
monitor foreign visitor activities for indications of their targeting of company personnel.
report suspected targeting as early as possible to minimize potential problems.

Robert H.Conley
Security Specialist
DOC/Western Region Security Office