The Internet

The Fastest Growing Modus Operandi for Unsolicited Collection

Based on reports of suspicious foreign contacts submitted to the Defense Security Service (DSS), the Internet is the fastest growing modus operandi of unsolicited correspondence using computer elicitation between foreign entities and cleared U.S. companies and their employees. Reports continue to arrive at DSS about foreign entities using the Internet to contact a wide variety of knowledgeable persons, with the intention to collect various pieces of information from each based upon their area of expertise. This information is then put together in an amazingly clear mosaic, revealing a level of detail that no one individual would have been able to provide.

Use of the Internet offers a variety of advantages to a foreign collector. It is simple, low cost, nonthreatening, and relatively risk free for the foreign entity attempting to collect classified, proprietary, or sensitive information. These foreign entities can remain safe within their own borders while sending hundreds of pleas and requests for assistance to targeted U.S. companies and their employees. The unsolicited request for information, including use of the Internet, is the most frequently used modus operandi by "closed countries" and may often be worded to appeal to cultural commonalities.

- **Sample Case:** One recent Internet request, sent from a foreign entity to cleared U.S. contractors, was a blatant unsolicited request for references to military projects that use software tools for networked, real-time operating systems (airborne, space, missile, tactical, intelligence, etc.). In the request, the foreign entity acknowledged much of the information would probably be classified. He also acknowledged his foreign "military customer" was too classified to be directly involved in sending the request over the Internet, so he was performing the request as a service to the foreign government.
- **Sample Case:** In another report of suspicious activity involving the Internet, a cleared U.S. company received a request to market a software program, with intelligence applications, to intelligence and security organizations in an Eastern European country. The software program enables the quick integration of multiple data sources and millions of documents with incredible speed, and can be used as an investigative tool to search various Web sites. At a minimum, the software program can be used by foreign companies to acquire competitive business intelligence off the Internet.

In many foreign countries, access to the Internet is potentially through a government host. Any foreign contact with these countries via the Internet is subject to intelligence and security service vetting and monitoring to prevent the loss of technical secrets and collection and exploitation of western technology. Access to Internet search software will undoubtedly assist foreign intelligence and security services in searching and monitoring the Internet for both intelligence and counterintelligence purposes. In one East European country during the past two years, the number of Internet hosts have grown exponentially, making it more difficult to isolate intelligence officers attempting to use the Internet to break into U.S. computer systems. Foreign intelligence services are known to use computers to conduct rudimentary online searches for information, including visits to government and defense contractors' online bulletin boards or

Web sites on the Internet. Access to Internet advanced search software programs could possibly assist them in meeting their collection requirements.

While the use of advanced software tools by foreign intelligence and security services is inevitable, security lessons can be learned from these reported incidents and we can implement security countermeasures to mitigate demonstrated vulnerabilities. We know foreign entities use the Internet because it provides an easy, low-cost, risk-free means to solicit information. We also know foreign intelligence and security services monitor the Internet and have the advanced software tools to make their searches and investigations much easier.

All requests for information received via the Internet should be viewed with suspicion. Only respond to people who are personally known and only after verifying the identity and address of the requester. Verification is important, as the possibility exists for foreign entities to present themselves as impostors. If a request is received from an unknown source or is not in character with the nature of requests normally made by a known source, a copy of the request should be provided to the security office and the request should not be responded to in any way.

The following is a list of suspicious indicators of foreign collection efforts via computer elicitation:

- The address is in a foreign country.
- The recipient has never met the sender.
- The sender identifies his/her status as a student or consultant.
- The sender identifies his/her employer as a foreign government, or states that the work is being done for a foreign government or program.
- The sender asks about a technology related to a defense-related program, project, or contract.
- The sender asks questions about defense-related programs using acronyms specific to the program.
- The sender insinuates the third party he/she is working for is "classified" or otherwise sensitive.
- The sender admits he/she could not get the information elsewhere because it was classified or controlled.
- The sender advises the recipient to disregard the request if it causes a security problem, or the request is for information the recipient cannot provide due to security classification, export controls, etc.
- The sender advises the recipient not to worry about security concerns.
- The sender assures the recipient that export licenses are not required or not a problem.