Host Security Briefing for Foreign National Guests

(To be given to DOC Agency Personnel in the area of the FNG)

Long-term foreign visits to U.S. national laboratories, government contractors, and other companies or research laboratories in the private sector can pose a serious threat to national security.

Given access to U.S. scientific, technical, or other proprietary information, foreign experts can gain for their home country information that may erode the U.S. lead in commercially advantageous technologies and critical military technologies. Often the difference between the technology used in unclassified research and a classified weapons program is only the "application" of the technology.

Foreign scientists and engineers sometimes offer their services to research facilities, academic institutions, or defense contractors. This can be an effort to place a foreign national inside the facility to collect information on the technology available there. Some prominent foreign scientists who obtained employment with U.S. companies have immediately sent acquired information via fax transmissions back to their former associates in their home country, using their native language so the U.S. company could not monitor what was being sent.

In some instances, foreign graduate students in the US have been asked by their government or a national corporation to serve as assistants at no cost to professors doing research in a targeted field. The student then has access to the professor's research and learns the applications of the technology.

Some foreign governments routinely task their graduate students in the United States to acquire information on a variety of economic and technical subjects. In some instances, the students are contacted and recruited before they come to the United States to study. Others are approached after arriving and are recruited or pressured based upon a sense of loyalty or fear of their home country's government or intelligence service. The security officer of a cleared U.S. defense contractor reported the company's desire to employ the son of a prominent foreign scientist from a European country. A name check of the scientist revealed he had previously cooperated with his country's foreign intelligence service.

One allied foreign government has an organized program to send interns abroad as an alternative to compulsory military service. In return for exemption from military service, the intern has the specific task of collecting foreign business and technological information.

The following indicators should trigger security concern:

- Foreign applicant has a scientific background in a specialty for which his country is known or suspected to have a collection requirement.

- The technology the individual wants to conduct research on may have classified applications (dual use technology), be on the militarily critical technology list, or be export-controlled technology.
- Foreign intern (student working on masters or doctorate) offers to work under a knowledgeable individual for free, usually for a period of 2-3 years. If any foreign national applicant offers services for free, the foreign government or a corporation associated with the government may well be paying the expenses and expect to gain accordingly.

Without sustained security and counterintelligence awareness training programs, assimilation of foreign personnel into the work environment usually results in a relaxation of security awareness among U.S. employees. Security compromise is a frequent result.

Host Security Briefing for Foreign National Visitors

(To be given to Agency Personnel in the area of the FNG)

The United States encourages technical information exchanges with scientists from foreign countries, as much can be gained from international collaboration. Most of these visitors are here as our guests at our request. Obviously most visitors are not engaged in intelligence work. They do only what they were invited to do. The problem is that in such a flood of visitors, it becomes hard to detect those who do come with ulterior motives. Without appropriate security precautions, it is possible to lose a great deal of classified, proprietary, or otherwise sensitive information.

Inappropriate or suspicious activity by foreign visitors to U.S. commercial or defense installations is a common occurrence. With few exceptions, security compromises reported from foreign visit incidents could have been prevented if U.S. personnel had been properly briefed in advance of the visit as part of the risk management process.

Below are some commonly used tactics by foreign national visitors to circumvent US security restrictions:

Hidden Agendas

Visitors sometimes pursue an agenda different from the stated purpose of the visit. That is, they arrive to discuss program X but do everything possible to discuss, observe, or meet with personnel who work with program Y. They exploit our natural habit of being courteous to visitors.

Wandering Visitors

A foreign visitor separates from the escorted party and strays "accidentally" into other areas of the facility.

Embarrassing Incidents

When confronted about attempts to wander from the escorted party or to elicit information beyond the approved scope of the visit, visitors sometimes feign indignation and deliberately create an embarrassing scene. Too often, the host attempts to be conciliatory, giving the visitors opportunities to fulfill collection objectives.

Unannounced Changes

Last minute or unannounced changes to add personnel or substitute personnel may be an attempt to sneak an intelligence officer or technical expert (in a technical area that is not supposed to be a subject of the visit) into the visiting party.

Exploiting the Foreign Visits System

The U.S. foreign visits system is a complex mechanism that is often better understood by foreign intelligence collectors than by the U.S. organizations that participate in the system. One way to exploit the system is to make multiple requests to different U.S. agencies. Another is to take advantage of different procedures depending upon whether the visit can be described as government sponsored, non-sponsored, or commercial in nature. For example, if a classified visit is disapproved, the foreign group may seek to arrange a commercial visit through a different U.S. Government agency.

Exploiting Misinterpretations

U.S. personnel often fail to understand the limitations of government sponsored and non-sponsored foreign visits. For government-sponsored visits, the contractor personnel may be under the impression that any inquiry by the foreign visitor is legitimate. For non-sponsored visits, the fact that the U.S. Government did not forbid the visit and the foreign visitors forwarded security clearances may give the U.S. contractor personnel the mistaken impression that it is okay to discuss sensitive or classified information.

Foreign Video Film Crews

Requests for foreign film crews to make documentary films are increasing, and a number of these requests have been quite suspect. Reports from U.S. industry have identified attempts at filming sensitive equipment and documents, as well as attempts at technical interrogation of subject-matter experts as part of an “interview”.

Improvised Technical Penetration

Foreign national visitors may use common, commercially-available technology to enhance their ability to circumvent U.S. security controls. Cell phones, Personal Data Assistants (PDAs), digital cameras, and pen drives can all be used to surreptitiously acquire sensitive or even classified information. A cell phone camera may be used to surreptitiously photograph documents or equipment. A pen-drive can download the contents of a hard-drive into a small, easily concealed device. Some PDAs combine the features of a cell phone with that of a small computer. These items are very common and may not be perceived as posing a threat by U.S. personnel.