

University of California (UC) Briefing for UC Visits to the People's Republic Of China

Background: Classification and Export Controls:

The United States controls the dissemination of technical information about technologies that may pose a threat to the national security in two ways: (1) through classification of information and classified research in cleared facilities; and (2) through export regulations that require licenses for the shipment of goods to certain countries as well as licenses to transfer technical data (blue prints, designs, drawings) about the goods to foreign nationals inside the U.S.

In the case of the export regulations, there is a safe harbor for academic research conducted in a University setting. Specifically, when technical data about controlled technologies results from fundamental research and the resulting information is shared broadly within the academic community, no license is required to disseminate the technical data to foreign nationals. Accordingly, a commercial contractor may be required to secure an export license to transfer the technical data to a foreign person (because the commercial contractor is treating the data as a trade secret and not publishing or openly sharing the data), while the University can disseminate the same type of technical data to a foreign person without violating the export regulations.

Indeed, the University's compliance program for export regulations is to assure that technical data about controlled commodities is being openly shared and published, thereby obviating any need to secure a license for the transfer of such technical data to foreign persons whether in the U.S. or abroad.

Export Regulations:

To comply with export regulations (whether under the Export Administration (EAR) or International Traffic in Arms (ITAR)), the University must structure the research relationship such that all the resulting scientific advancements are openly shared in the academic community. Accordingly, trade secrets from Chinese companies cannot be received, and there can be no agreement to keep research results confidential or to limit disclosure of the findings for a period of time. The research environment must be open; that is, nationals from other countries must be able to participate in the project and nationality, citizenship or Visa status cannot be a criterion for project participation.

Classified Information:

There is no equivalent exception for fundamental research in the classified area. All classified information must be protected from disclosure and as such cannot be disclosed to uncleared foreign nationals. While certain members of a UC delegation to the PRC may hold a security clearance because of their role in operating or oversight of the DOE Laboratories, in most cases specific classified information has not been provided to these cleared individuals holding a UC management or Regent position (unless, of course, the individual is a bench scientist actually conducting classified research). If you have any question about what classified information you have received and what steps you must take to protect the information, please contact the OP Security Officer, Willie Archie at willie.archie@ucop.edu.

The following further describes tactics used by the Chinese to gain access to classified information.

China's Acquisition of Technology:

The FBI has identified China as one of the most aggressive collectors of technology and secrets. According to the FBI, China uses its nationals who are sent to North America to study advanced technology to infiltrate U.S. companies to gain access to sensitive information. They then return to China and set up their own companies or provide the information to the military.

Intelligence officials indicate that one of China's common methods is to use visiting students, scientists, businesspeople, and even trade delegations to obtain sensitive material. Recent cases, currently winding through the courts, reveal that natives of China have been accused of obtaining technology from Silicon Valley companies with the intent of exporting it to China.

The Cox Committee's assessment is that China's technical advances have been made on the basis of classified and unclassified information derived from espionage, contact with U.S. and other countries' scientists, conferences and publications, unauthorized media disclosures, declassified U.S. weapons information, and Chinese indigenous development. The relative contribution of each cannot be determined.

The American research scientist should be mindful of the various ways of elicitation employed by the intelligence arms of the Peoples' Republic of China that may tempt the American researcher to violate our Export Control laws.

Elicitation Techniques

General Elicitation Strategy:

1. Keep you comfortable while pursuing clandestine approaches to eliciting information.
2. Discreetly ask you for extra bits of information
3. Will push you to discuss denied areas of information: "Someone as smart and accomplished as you must know how much you can share with us without harming the security of the U.S."
4. Will seek information from you over a long time frame, as necessary to obtain the information they desire.
5. Will validate the same information from other sources.

Manipulation of the Physical Environment to Induce the Loss of Information:

1. Will induce fatigue—Travel Guide may take you to an all day excursion knowing that you must deliver a lecture in the evening to distinguished guests.
2. At an evening banquet in your honor added alcohol will impair your judgment when 10-12 individuals make toasts in your honor, at which time 10-12 other people will surround you with questions, separating you from your companions.

Psychological Techniques of Elicitation:

1. “Priming the Pump”: “...I probably shouldn’t tell you this, but XYZ is the equation for the bomb!” [They want you to correct them and advise that it is missing certain other elements to be accurate].
2. Make a Fuss over you: “Holding a banquet in your honor and/or present awards to you.” Bring in prominent national experts to hear you speak; inviting you to deliver a more substantive and informed speech to impress their national experts rather than the informal talk you had planned.
3. Instead of presenting you in a small graduate student lounge within the University, your speech takes place in the Great Hall of the People where there are hundreds in the audience.
4. Will disarm you “...China is a poor and bankrupt nation not in position to harm the U.S. If we all work collaboratively together, we each can achieve our national objectives.”
5. Will prompt you “...I have a problem with XYZ. What can you tell me about solving this problem?”

Reciprocity:

PRC exploitation operations tend to be repetitive and fall into the same pattern as described above. Avoid the ‘hotspots’ and you most likely will avoid any loss of information due to elicitation. Also be aware that your hosts will be anticipating a return visit invitation to your facilities (National Labs, etc.) whereby they might continue their elicitation exploitation operations.

Summary:

American universities may engage in collaborative research activities with institutions within the People’s Republic of China and within other countries, even though such countries are on the DOE/NNSA “Sensitive” Country” listing. National policy recognizes that an open university, where results are disseminated and published, serves the national interests and creates advancements that may then be applied in a classified setting. It is recognized that conducting open, fundamental research makes a valuable contribution to the economic and national security interests of the United States, as does the conduct of classified research. While entering into collaborative research arrangements is by nature the fundamental right and pursuit of any American university, an issue of critical importance to our national security is safeguarding our nuclear secrets and other classified data. The purpose of this briefing paper is not to discourage research opportunities within the PRC or other countries, but to remind the American researcher that he or she must not disclose controlled information prohibited by U.S. law, and must also safeguard classified information. However, export controlled information generated in the university research environment may be shared as long as we are not sharing such technical data on a preferential basis and the technical data is also being openly shared with others and published.

Acknowledgement of Briefing

To: University Research Security Officer
Laboratory Administration
1111 Franklin Street, 5th Floor
Oakland, CA 94607-5206

Receipt of a copy of this Defensive Briefing paper on the People's Republic of China sent to me with regards to my trip to China is hereby acknowledged:

Date: _____

Print Name: _____

Signature: _____
