Academic Solicitation Security Briefing

NEW MEXICO TECH

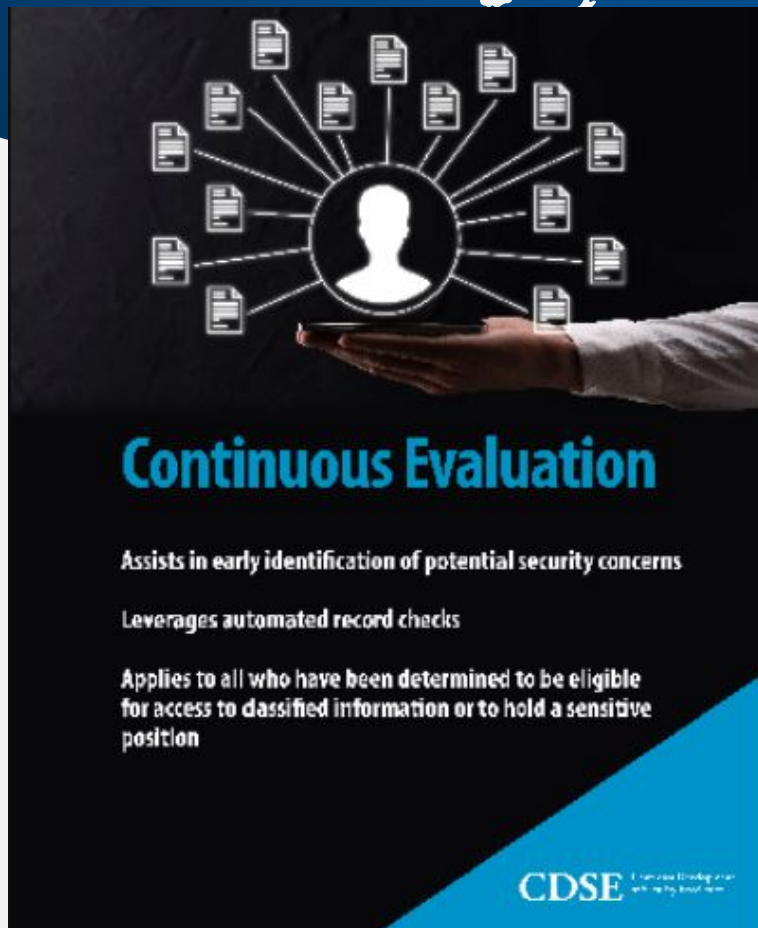
Introduction



The purpose of this briefing is to provide an awareness of the solicitation of academia to exploit individuals and gain access to sensitive or classified information and technology. Adapted from the DCSA Academic Solicitation brochure and the 2019 Targeting U.S. Technologies report.

Foreign intelligence entities exploit unsuspecting professors and researchers to gain access to sensitive or classified information and technology.

Placing academics at, and requesting to collaborate with U.S. research institutions under the guise of legitimate research offers access to developing technologies and cutting-edge research, any such placement and information learned would not only satisfy the collectors; immediate technological requirements, but also result in better educated scientists and researchers for indigenous technology development.



What is Academic Solicitation?

Academic solicitation is one of the fastest growing methods of operation reported by cleared contractors. The number of foreign academics requesting to work with classified program continues to rise, and the academic community will likely remain a top target for the foreseeable future.

Defense Counterintelligence and Security Agency (DCSA) defines academic solicitation as the use of students, professors, scientists or researchers as collectors improperly attempting to obtain sensitive or classified information. These attempts can include requests for, or arrangement of, peer or scientific board reviews of academic papers or presentations; requests to study or consult with faculty members; requests for and access to software and dual-use technology; or applications for admission into academic institutions, departments, majors, or programs, as faculty members, students, fellows, or employees.

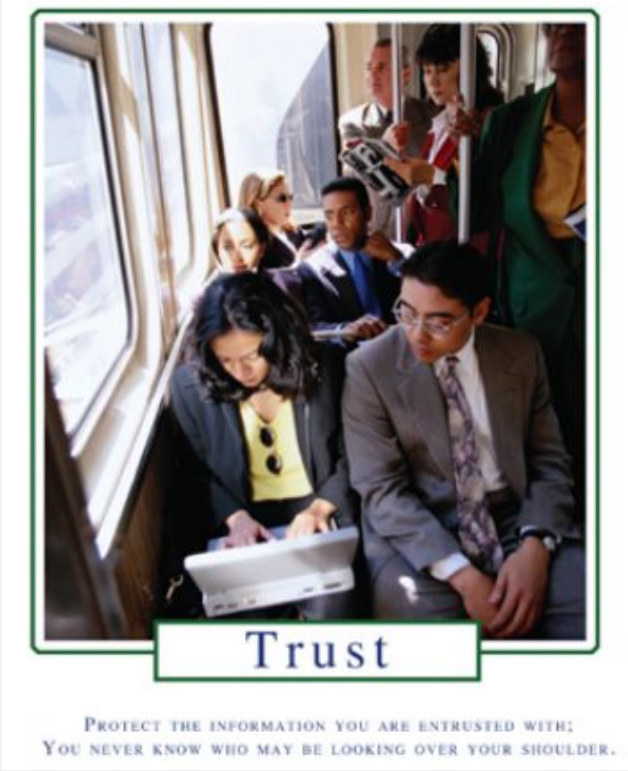
Most of these contacts are likely legitimate. However, some foreign academics may ultimately take advantage of their placement and access to further national research and development goals. In such cases, foreign nationals studying under or regularly interacting with cleared employees engaged in classified research and development pose a threat to U.S. government sponsored basic and applied research.

It is imperative for academics to be familiar with, and comply with, the laws, regulations and procedures governing the restrictions on sharing classified, or export-controlled, technologies and information with foreign students or academics.

Who is Being Targeted?



- Subject matter experts teaching technical courses
- Researchers and scientists conducting classified research on behalf of a U.S. government customer
- Researchers, scientists and subject matter experts, employed at cleared components of academic institutions
- Researchers, scientists, and subject matter experts with unclassified work published in scientific or technical journals or presented at science conferences



What Are They After?

- Classified, sensitive, or export-restricted basic and applied research
- Developing defense or dual-use technologies
- Information and students, professors, and researchers working on the technologies



Why is it Effective?

- Academic solicitation is an effective way of collecting information due to the collaborative nature of the academic community.
- U.S. universities and research institutions regularly host foreign students to help cultivate their technical abilities without realizing that this free-flowing exchange of information can place the U.S. technological infrastructure at risk. Home countries can expect their student's access to supplement intelligence collection efforts against emerging U.S. DoD and civilian technical research.
- U.S. researchers that receive unsolicited requests to review scientific publications readily provide feedback with the hopes of reviewing the resulting findings. However, any feedback provided may confirm or refute scientific hypotheses.
- Foreign intelligence entities use foreign students who are already knowledgeable about targeted academic fields to collect.
- Foreign students and professors target U.S. students and researchers who are knowledgeable in the desired field.
- It is often difficult to discern the legitimate contacts from those that represent nefarious attempts to gain access to sensitive or classified information or technology.

Common Scenarios



- Foreign students accepted to a U.S. university or to postgraduate research programs are recruited by their home country to collect information, and may be offered state-sponsored scholarships as an incentive for their collection efforts
- U.S. researchers receive requests to provide dual-use components under the guise of academic research
- U.S. researchers receive unsolicited emails from peers in their academic field soliciting assistance on fundamental and developing research
- U.S. professors or researchers are invited to attend or submit a paper for an international conference
- Overqualified candidates seeking to work in cleared laboratories as interns
- Candidates seeking to work in cleared laboratories whose work is incompatible with the requesting individual's field of research
- Intelligence entities will send subject matter experts (SME's) requests to review research papers, in hopes the SME will correct any mistakes

What to Report

Any contact (i.e., emails, telephone, personal contact) that is suspicious because of the manner or subject matter of the request. This may include requests from U.S. persons, or from foreign nationals located in the United States or abroad, and may consist of:

- Unsolicited applications or requests for undergraduate, graduate, postgraduate or other research positions
- Unsolicited requests for access to research papers or other research-related publications or documents
- Unsolicited requests for assistance with or review of these papers, draft publications or other research-related documents
- Unsolicited invitations to attend and/or present at international conferences





Key Findings from FY18 Cleared Industry Reporting



- The number of reports assessed to be a suspicious contact increased by 3 percent over FY17
- The top four most targeted technologies in FY18 were in the top five most targeted technologies in FY17

  Optics was the fifth most targeted technology; previously it had not been one of the top five
- East Asia and the Pacific was the most commonly identified origin of incidents reported by cleared industry
- Attempted acquisition of technology was the most common MO.
- Exploitation of cyber operations increased by 55 percent in FY18.
- Email was the most common MC used in 41 percent of the reported incidents
- Phishing operation was the second most common MC used in 9 percent of the incidents
- Cleared industry reporting also noted foreign collection targeting services provided by cleared industry

BE ALERT! BE AWARE! Report suspicious activity to the Security Office!

NEW MEXICO TECH