

Senator Cornyn Questions for the Record
For Dr. Kevin Gamache, Chief Security Officer, Texas A&M University System:

- 1. In your written testimony you state that researchers who participate in foreign talent recruitment programs present a “significant vulnerability by providing an enhanced opportunity for the inadvertent or purposeful sharing of controlled information.” Given your experience in this area, could you expound on that observation?**

When students and visiting scholars participating in foreign talent recruitment programs from countries of concern are given access to labs at U.S. universities, they can also gain access to research data and results available to their U.S. Citizen colleagues. The access to university information systems, laboratories, and research personnel can all provide an opportunity for someone being directed by an outside agency to serve as a “non-traditional collector” and remove research data and results from the labs to which they have access.

An Academic Counter Exploitation working group such as suggested in the recommendations of my written testimony could serve as a method to carefully consider and make recommendations on how policies could be put in place that both educate the faculty, allows for open exchange where appropriate, and protect the information that needs to be protected.

- 2. Do you have concerns about allowing individuals participating in foreign talent recruitment programs to take part in sensitive U.S. government-sponsored research projects?**

Most definitely. Allowing such access to sensitive U.S. government-sponsored research could put the technology at significant risk. Open source literature on foreign talent recruitment programs suggests that participants are being tasked to help meet the technology needs of our adversaries by taking research from U.S.-based labs. Stealing this research or technology allows our adversaries to “leapfrog” the United States in technology development instead of investing in their own research.

Many U.S.-based researchers are naïve to the methods and intent our foreign adversaries are using to gain access to our sensitive technology. The result is that they become unwitting participants in these talent platforms. One of the key roles an Academic Counter Exploitation working group could play is to inform U.S. faculty and graduate students regarding these talent platforms.

- 3. Are foreign talent recruitment programs something you have addressed within the Association of University Export Compliance Officers and at the Texas A&M Academic Security Conference?**

While I am a member of the Association of University Export Compliance Officers, I cannot speak for the organization and would refer you to the leadership of AUECO for comment. For the last six years, however; I have managed a listserv of Facility Security Officers from universities participating in the National Industrial Security Program (NISP). There are

approximately 120 universities active on this list serve. For the past two years, Texas A&M has sponsored an academic security conference for those same NISP participants. In 2018 more than 65 schools participated. The topic of foreign talent recruitment platforms is a frequent source of discussion in both of these forums. One of our featured speakers at the 2018 Academic Security Conference was Mr. Dan Golden, author of “Spy Schools” who touched on the use of talent programs by our foreign adversaries to gain access to university labs. We also had Mr. Allen Phelps from Threat Farm, LLC who presented a comprehensive briefing to participants on the Talent Platforms and how they are used by nation-states to get access to sensitive technology.