Dr. Kevin R. Gamache
The Texas A&M University System
U.S. Senate
Subcommittee on Border Security and Immigration of the Judiciary Committee
"Student Visa Integrity: Protecting Educational Opportunity and National Security"
Dirksen Senate Office Building, Room 226
Wednesday, June 6 at 2:30 pm

Introduction

Chairman Cornyn, Members of the Subcommittee, thank you for the opportunity to testify before you today.

I come before you this afternoon as the Chief Research Security Officer (CRSO) of The Texas A&M University System to discuss the unique challenges of protecting our nation's cutting-edge technology and maintaining our national security in the free and open environment of academia.

The Texas A&M University System (TAMUS) is one of the most extensive systems of higher education in the nation, with an annual budget of $4.7 billion. Through a statewide network of 11 universities and seven state agencies, the Texas A&M System educates more than 152,000 students and makes more than 22 million additional educational contacts through service and outreach programs each year. System-wide, research and development expenditures exceeded $972 million in FY 2016 and helped drive the state's economy.

Texas A&M (TAMU) places significant value on global engagement. The flagship of the A&M System is proud to be the choice of many international students from over 127 countries. Further, more than 3,800 students, the most of any public university in the United States, participate in study or work abroad opportunities. Our undergraduates discover ways to serve and impact communities around the world, all while participating in real-world learning communities through our international study abroad programs. We believe that international engagement provides crucial transformational learning for our students that does not just impact them, it affects the world. We are also home to a global network of scholars in our faculty who contribute to our research, teaching and scholarship missions. Texas A&M has a long history of cooperation and collaboration with global partners to build educational programs, conduct critical research, and develop innovative solutions for global problems. Texas A&M currently has approximately 275 active international agreements with about 60 countries around the world. Finally, we have more than 440,000 living former students, many of whom are hard at work worldwide in more than 150 nations.

My responsibilities as CRSO include providing management and oversight of all classified research, controlled unclassified programs, and export-controlled research being conducted by A&M System members. These responsibilities include; development of system policy for managing controlled access programs; working with A&M System member compliance and export control offices to vet visiting scholars; providing assessments and assistance regarding physical

and personnel security associated with our controlled research contracts; and management of our controlled access facilities.

The A&M System has been a member of the National Industrial Security Program (NISP) since 1974. Executive Order 12829 established NISP to ensure that cleared US defense industry partners safeguard classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. As a NISP participant, the A&M System is a cleared defense contractor just like Lockheed Martin, General Dynamics, or the more than 13,000 other NISP participants upon whom our national security depends. The A&M System has been granted Facility Clearances by the Department of Defense and Department of Energy, and we currently conduct classified research for both organizations from our facilities at the flagship campus in College Station.

As I speak about Texas A&M and what we do to protect our security, it is important to note that many universities have different security needs that may not be as great as those that exist on our campus. Because many of our sister institutions choose not to conduct classified or export controlled research projects, or if they do, they perform this research off campus at separate secured facilities, their security requirements may be substantially less than ours.

The A&M System's security program has amassed a record of six straight SUPERIOR ratings during annual Security Vulnerability Assessments conducted by the Defense Security Service (DSS). The DSS recognized the A&M System with a 2015 Colonel James S. Cogswell Outstanding Industrial Security Achievement Award as one of 41 from more than 13,000 defense contractors subject to recurring security assessments. The award recognizes those security programs that far exceed basic NISP requirements and provide leadership to other cleared facilities in establishing best practices while maintaining the highest standards for security. More recently the DSS recognized the A&M System with their 2017 Award for Excellence in Counterintelligence We appreciate Senator Cornyn joining DSS in awarding TAMUS this significant award on campus in March. Texas A&M was one of just two facilities out of more than 13,000 entities to receive the award last year in recognition of those contractors and universities who best demonstrate the ability to stop foreign theft of US defense and national security technology.

Background

The A&M System's Research Security Office provides security oversight for all 18 system members, but because of the amount and type of research conducted at certain places, we pay particular attention to four system members. Those are:

TEXAS A&M UNIVERSITY— The flagship university of the A&M System, is a tier one research institution and the State of Texas' land grant institution, which opened in 1876. This university has strategically grown into one of the nation's most comprehensive universities, offering 430 bachelor's, master's, doctoral and professional degree programs through 16 colleges and schools, including the School of Law in Fort Worth, and the health-related programs of the

Health Science Center together with two special-purpose branch campuses in Galveston and Doha, Qatar. Texas A&M also has global reach through our study centers in Mexico, Italy, and Costa Rica.

TEXAS A&M AGRILIFE RESEARCH – AgriLife Research is the state's leading public agency for research and development in agriculture, natural resources, and the life sciences. With a statewide presence – from its headquarters in College Station to other A&M System campuses and at 13 regional Research and Extension Centers – the agency provides innovative solutions to 21st-century challenges. Its goals are to enhance competition and prosperity in agriculture, sustain healthy ecosystems and conserve natural resources, improve public health and well-being, and optimize plant and animal production and human health. Because Texas's unique climatic and geographical diversity make it a microcosm of geographic regions worldwide, the impacts of AgriLife Research's discoveries extend far beyond Texas borders. AgriLife Research collaborates with state and federal agencies, private-sector corporations and international organizations from more than 30 nations.

TEXAS A&M ENGINEERING EXPERIMENT STATION (TEES) – For more than 100 years, TEES has served the citizens of Texas, and the nation, through engineering and emerging technology-oriented research and educational collaborations. TEES partners with industries, communities, government agencies, community colleges and universities to find solutions to improve quality of life, foster economic development and enhance education. TEES also helps improve the workforce by engaging over 1,500 undergraduate and graduate students in research each year. Research activities focus on essential needs in areas including energy systems and services, safety and security, healthcare, materials and manufacturing, information systems and sensors, industry outreach and education and training. The TEES state agency headquarters is in College Station and specialized research centers and partner institution offices throughout the state of Texas. In addition, TEES researchers are at the forefront of some of the most cutting-edge research happening in the world today. TEES has extended its reach globally, having established relationships with countries such as Mexico, Brazil, Japan, Greece, France, India, Argentina and Qatar.

TEXAS A&M TRANSPORTATION INSTITUTE (TTI) – This state agency develops solutions to the problems and challenges facing all modes of transportation. TTI is one of the premier higher education-affiliated transportation research agencies in the world. TTI research is widely known as an excellent value with a proven impact of saving lives, time and resources. Located on the campus of Texas A&M University in College Station, TTI maintains a full-service safety proving grounds facility; environmental and emissions facility; and sediment and erosion control laboratory at the A&M System's RELLIS Campus in Bryan, Texas, which is home to the new A&M Center for Infrastructure Renewal and visited earlier this year by US Energy Secretary Rick Perry. TTI has eight offices in Texas, as well as Washington D.C., Mexico City, and Doha, Qatar.

Role of Academia in Protecting the Nation's Technology Assets

In 1982, The Panel on Scientific Communication and National Security was asked to examine the various aspects of the application of controls to scientific communication and to suggest how to balance competing national objectives and to best serve the general welfare. The National Academies produced a Consensus Study report entitled *Scientific Communication and National Security*[1]. Based in part on the NAS report, the Reagan Administration issued National Security Decision Directive 189[2]. This national security decision directive was vital because it firmly established classification of research as the primary mechanism to be used by the government to control research with national security implications. It also sought to ensure that "fundamental" scientific research, to the maximum extent possible, remain unrestricted to promote the openness required for scientific advancement.

In a 2001 letter reaffirming NSDD 189[3], then Secretary of State, Condoleezza Rice stated: "The key to maintaining US technological preeminence is to encourage open and collaborative basic research. The linkage between the free exchange of ideas and scientific innovation, prosperity, and US national security is undeniable. This linkage is especially true as our armed forces depend less and less on internal research and development for the innovations they need to maintain the military superiority of the United States."

The terrorist attacks on September 11, 2001, greatly exacerbated concerns about protecting research with national security implications. In 2005, the Center for Strategic and International Studies explored this topic in their white paper, *Security Controls on Scientific Information and the Conduct of Scientific Research: A White Paper of the Commission on Scientific Communication and National Security*[4]. The paper noted "Scientific and technological accomplishments – and a workforce trained to exploit them – are necessary to defend the nation and enhance its quality of life." The study also noted these accomplishments tend to be published openly and thus become available to all. Open communication and participation are fundamental to the conduct of high-quality research, as this openness allows for anyone to critique and validate (or disprove) research results, and "fosters the dynamic and often serendipitous interaction from which successive innovation can arise…"

The study goes on to discuss the understandable and necessary desire for policies that limit the ability of those with malicious intent to access and exploit scientific research. However, it also indicates that while such policies may have the effect of constraining participation in, and dissemination of, specific research, they can also have the deleterious effect of hampering the critical evaluation and dynamic interactions discussed above. Further, it noted that due to the global nature of economy "…unilateral national policies to control scientific and technical information may have little prospect of effectively doing so."

In 2007, the National Research Council published a report on this topic, *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security*

[1] https://www.nap.edu/catalog/253/scientific-communication-and-national-security
[2] https://fas.org/irp/offdocs/nsdd/nsdd-189.htm
[3] https://fas.org/sgp/bush/cr110101.html
[4] https://www.csis.org/analysis/security-controls-scientific-information-and-conduct-scientific-research

Communities[5]. This report states, "Therefore, developing and implementing measures to control access to sensitive information must be considered within the context of overall costs to the research community, and to the public that benefits from the results of such research, and with an eye toward the anticipated effectiveness of such measures to actually enhance security." Jack Gansler, former Defense Undersecretary for Acquisition, Technology, and Logistics was a chair of the committee that wrote this report, along with Alice Gast, former VP for Research at MIT.

In 2009, the National Research Council published another Consensus Report on this topic entitled, *Beyond "Fortress America*[6]*"* which warns, in an attempt to maintain superiority, we can quickly implement policies that make us less competitive and thus weaken our national security. Brent Scowcroft, US National Security Advisor under US Presidents Gerald Ford and George H. W. Bush was a co-chair of the committee which wrote this report along with John Hennessy, then president of Stanford University.

In light of these previous reports, as we discuss policy for the regulation of sensitive research, we must be mindful of the importance of our ability to compete on the global stage, to have research robustly evaluated, and to draw on and synergize with the best and brightest internationally. Regulations and policy in this area must be crafted carefully, and implemented only in those situations where it can be effective, and outweighs any associated penalties.

Defining the Threat

Because of the recognized strengths of US universities, particularly in Science, Technology, Engineering, and Mathematics (STEM) fields, our universities have been primary destinations for a significant number of international students and visiting scholars in recent years. Texas A&M is proud to host many such individuals. In general, this global engagement has been positive, as discussed above, fueling innovation and discovery through basic research collaboration and providing the US workforce with much-needed talent when these students graduate and become employed in the US.

This global engagement can also present vulnerabilities at university campuses, however; and the academic community must be vigilant in protecting controlled information. Gaining access to US institutions of higher education involved in sensitive and critical defense-related research offers the opportunity for our adversaries to bridge gaps in their current technical knowledge. It also allows other nations to avoid the costs of conducting basic research. Capitalizing on US research investments in this manner enables our adversaries to leapfrog the US in innovation and can be a threat to US national security.

Talent recruitment programs have recently come under scrutiny as a method for foreign entities to acquire sensitive information from academic institutions. Talent recruitment programs use multiple incentives to recruit global industry and university experts to work for the foreign entity in critical areas deemed essential to developing their most important technical requirements.

[5] https://www.nap.edu/catalog/12013/science-and-security-in-a-post-911-world-a-report

[6] https://www.nap.edu/catalog/12567/beyond-fortress-america-national-security-controls-on-science-and-technology

While not illegal, associating with these programs presents a significant vulnerability by providing an enhanced opportunity for the inadvertent or purposeful sharing of controlled information.

Best Practices in Academia to Confront the Threat

Concerns over the intersection of national security and science existed before and during the Cold War. The terrorist attacks on September 11, 2001, created new worries about who is conducting research on the campuses of US universities. Since that time, international students and faculty have faced stricter scrutiny from the federal government before being admitted into the US. Additionally, universities have become more vigilant about the security of research facilities and research programs and have taken additional measures to ensure compliance with rules relating to export controls, dual-use research, and classified information. Indeed, many universities have designated staff such as security officers and export control officers to more effectively ensure compliance with the laws and regulations in this area.

Export control regulations cover shipment of controlled physical items that require export licenses from the US to a foreign country and transfers of controlled information, including technical data. Universities must also comply with federal regulations when faculty and students travel to certain sanctioned or embargoed countries for purposes of teaching or performing research. Compliance with these and other regulations requires constant attention, particularly in an academic environment. Thus, at the national-level, new professional organizations have been formed to provide training and support. One such organization is the Association of University Export Compliance Officers (AUECO). Membership in AUECO is open to export control officers and other employees at institutions of higher education in the US who are responsible for the administration of export, import and trade sanctions regulations for their institution. Formed in 2008, AUECO currently consists of more than 200 members from over 140 different universities.

The A&M System has taken a leadership role in the academic community when it comes to addressing the unique challenges of maintaining an industrial security program for conducting classified research in the open environment of academia. We established the first Academic Security Conference in 2017 to provide a forum for those academic institutions participating in the NISP to benchmark and share best practices from their respective programs. The three-day conference features classified and unclassified presentations from DSS, Department of Commerce Bureau of Industry & Security, State Department Office of Defense Trade Controls, Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS). The conference is unique in that it focuses solely on the challenges of protecting classified and controlled unclassified information within the open environment of academia. We completed our second conference in March 2018 with over 60 universities participating. The A&M System will continue to host this conference annually, and we have already begun planning for our 2019 meeting.

While the Academic Security Conference provides an opportunity for academic security professionals to come together physically once a year, we have also established an ongoing platform for virtual collaboration. In 2012, we created a listserv for security professionals in academia to seek advice, benchmark, and share best practices on a daily basis. The listserv currently has over 120-member universities and remains extremely active. We also established the Academic Coun-

ter Exploitation (ACE) Program as a secure portal on the DHS's Homeland Security Information Network to allow academic institutions to share controlled unclassified threat information unique to academia. The program currently has 65 schools participating.

The A&M System established a System-level Research Security Office (RSO) in 2016 to provide program management and oversight of all classified research, controlled unclassified programs, and export-controlled research across the 18 A&M System members. The RSO manages the A&M System's relationship with DSS and members of the Intelligence Community that conduct business on our various campuses. The RSO provides a "one-stop" office for A&M System members to go to with security-related questions and issues. The RSO is also responsible for assisting with the vetting of visiting scholars and ensuring compliance with federal regulations on information and data security.

We have recently established a secure computing enclave to protect research funded by the federal government which contains controlled unclassified information. The secure computing enclave allows us to monitor the flow of information down to the project level and precludes anyone who might achieve unauthorized access to our secure computing enclave from gaining access to more than a single research effort.

While I have provided a few examples of areas where The Texas A&M University System is working hard to enhance our security posture, there are numerous other examples of universities taking equally commendable steps. I have included two such examples here.

The Purple Arrow Program instituted by the University of New Mexico, the Albuquerque Office of the FBI and DSS in 2008 has had a significant positive impact on the security community by providing support through a team of counterintelligence professionals from multiple agencies who have dedicated themselves to protecting classified and sensitive technology throughout New Mexico. This diverse group of professionals is composed of program leads for their respective agencies whose sole goal is to share information across agency boundaries. They consistently provide the most comprehensive threat information to the end user, which is most often the cleared defense contractor community.

Purple Arrow has created a daily newsletter that includes current news events relating to the insider threat, espionage, cybersecurity, and other similar topics that is distributed to over 7,000 recipients across the US to include cleared defense contractors, academic institutions, DoD agencies, US government agencies, and the White House Cyber Team. In addition to the daily newsletter, they distribute real-time threat warnings to the community as they arise.

Purple Arrow excels at sharing and oversight and has contributed immeasurably to the overall improvement of security procedures and practices within the community it serves. Due to their dynamic relationship and willingness to share information across agency borders, they continue to ensure the local security community has the most current threat information available. As a result, Purple Arrow is a top producer of cases and Intelligence Information Reports for law enforcement and the Intelligence Community.

The University of Kansas (KU) has also recognized the need to identify, reduce, and mitigate risks to its personnel, information, technology, and facilities as it collaborates internationally to fulfill its mission of education and research while protecting both its intellectual property and national security.

KU has created the Office of Global Operations & Security (GO&S) to better manage and reduce risk. The goal of GO&S is to create coordination and consistency in all areas related to KU's international, export controls, and security operations. GO&S will identify pertinent issues and provide strategic planning, advice and assistance to decision-makers, faculty, and staff on international operations, security, and other high-risk activities.

GO&S is staffed by employees with experience in international affairs, analysis, export compliance, security management, and the law. Areas of focus for GO&S include:

- International agreements, including research agreements
- International travel (students, faculty, and staff)
- International visitors (affiliates, visiting researchers, or scholars, etc.)
- International purchasing and shipping (customs regulations, international taxes)
- Export Controls and Compliance
- Cyber Security
- Information Security
- US Government Research Contracts and Grants
- Security Planning
- Liaison with Government and Corporate Partners
- University-wide Security Management

These are just a few examples demonstrating the fact that those of us in academia charged with protecting our research, our innovation, and our personnel have established a variety of means to coordinate, collaborate, and communicate across a wide variety of organizations to ensure success.

Recommendations for Future Actions

Many within the academic community are working diligently and having success protecting our national high-value research and intellectual property, but we can do more. We make the following recommendations:

- **Establish an Academic Counter Exploitation (ACE) Program Working Group.** This group should be comprised of those responsible for research security from strategically selected Tier I research universities. The group would work with the Federal Bureau of Investigation, the Defense Security Service and the Department of Commerce Bureau of Industry Security and be chartered by Congress to help inform policy solutions to counter the threat that foreign adversaries represent to sensitive research in US universities. Membership in the group would include those universities with a demonstrated record of excellence in industrial security and counterintelligence in academia. The Working Group would also manage the Academic Counter Exploitation Program as a national

initiative to inform faculty and administration at institutions of higher education on the threats to our research and innovation base.

- **Provide focused and robust funding for federal research and graduate students.** The talent recruitment programs mentioned previously would be much less effective if US faculty and students had reliable and sustainable resources to perform their research in and for the United States. If the US government matched the funding levels and provided a focus equal to what the Chinese government is contributing to their talent recruitment programs, that would propel the US ahead and diminish many of these issues considerably. Existing fellowship and scholarship for service programs have been highly successful at recruiting domestic talent into STEM graduate programs and could be expanded[7].

Conclusion

There is consensus within the academic community that "fundamental" scientific research should remain unrestricted to the maximum extent possible to promote the openness required for scientific advancement. Additionally, having the best and brightest students and scholars from around the world come to our institutions of higher education enhances our ability to innovate and create new knowledge, and to attract some of those superstars to make the US their home.

Nevertheless, we would be remiss if we did not also recognize the threat that such engagement inherently brings. The Defense Security Service assesses with high confidence that as long as the US remains a leader in research and development of advanced and emerging technologies, foreign collectors will target US technologies, in part, by encouraging their citizens to access US educational opportunities. Because of the potential for long-term technological and perhaps intelligence gain, foreign entities will very likely continue to use academic solicitations to gain access to US information and technology.

Accordingly, academic institutions must continue to work with federal agency partners to remain constantly vigilant of existing and evolving threats, to educate researchers about these threats, and to provide clear avenues for dealing with security-related issues. If we can do this, the collective US Academy will continue producing game-changing research, and the future workforce to execute it, while helping ensure that the US maintains its global technological and economic superiority.

[7] https://www.aau.edu/key-issues/national-defense-education-and-innovation-initiative