Questions for the Record
U.S. Senate Select Committee on Intelligence
Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center
Open Session
September 21, 2022

Dr. Kevin R. Gamache
Associate Vice Chancellor and Chief Research Security Officer
The Texas A&M University System

[From Senator Feinstein]

The U.S. Counterintelligence Enterprise

- **Which legal responsibilities should non-IC entities—including U.S. government agencies, academic institutions, and private sector companies—have to protect their intellectual property, research, technologies, and data with national security implications?**

  Academic institutions should have a legal responsibility to establish a policy that mandates the highest standards of integrity and compliance in ensuring the security of their member's research portfolios. This policy should establish the framework for (a) establishing a Research Security Office (RSO) as the responsible office for classified information, controlled unclassified information, management of the system's secure computing enclave, foreign influence reporting, and export controls, (b) achieving the highest level of compliance with applicable ethical, legal, regulatory, contractual and system standards and requirements in securing research portfolios, (c) promoting an organizational culture of compliance in meeting federal requirements to maintain federal funding, and (d) assisting members in related compliance operations.

- **Which incentives and resources could Congress provide to help non-Intelligence Community entities better protect their intellectual property, research, technologies, and data from foreign adversaries?**

  The CHIPS and Science Act (P.L. 117-167) authorizes the establishment of a research security and integrity information-sharing analysis organization (section 10338) and a regional secure computing enclave pilot program (section 10374(d)). Congress should appropriate funding to the National Science Foundation to establish these programs, in partnership with institutions of higher education with solid research security track records, to help academic institutions protect their intellectual capital, research, technologies, and data from foreign adversaries.

  Both initiatives would increase the ability of universities to collaborate more effectively regionally and nationally. They would also help to provide more limited, less well-resourced universities access to significant new capabilities for securing the research enterprise.

- **What are the biggest challenges academic entities face in confronting foreign adversarial intelligence collection and economic espionage?**

The US higher education system operates under a unique set of principles and commitments fundamental to the academy. Any attempt to secure the research enterprise must not compromise these principles, which include:

- Openness and transparency
- Accountability and honesty
- Impartiality and objectivity
- Respect
- Freedom of inquiry
- Reciprocity
- Merit-based competition

While these foundational principles are our greatest strengths, they can also present some of our most significant vulnerabilities, and therein lies the challenge. For example, our culture of openness can lead to potentially more substantial exposure to malign actors and risk. Our desire to collaborate with the brightest minds in the world might enhance the capabilities of some who do not share our fundamental values and national interests. Our world-class laboratories and equipment can provide access to world-class laboratories and equipment unavailable in most other countries. While this access can help solve the world's most challenging problems, it can also give greater exposure to risk. Our focus on pushing science to its limits can provide access to cutting-edge technology and scientific processes that others seek to emulate or acquire. Once again, this is not without some risk. Finally, institutional autonomy and academic freedom can make internal coordination difficult.

Each of these strengths makes our research enterprise effective and robust. As we implement measures to address risk in our institutions, we must ensure our solutions don't negatively impact our strengths. The challenge is how we achieve the proper balance.

- **Given the generally lawful nature of foreign acquisition of U.S. technology, does Congress need to consider additional updates to the Committee on Foreign Investment in the United States (CFIUS) to address the remaining loopholes?**

  The Committee on Foreign Investment in the United States (CFIUS) provisions are outside my area of expertise, so I cannot answer this question.

- **How can the U.S. government best strike a balance between protecting national security and preserving a culture of international collaboration, free enterprise, and open research?**

  One of the primary roles of academic institutions is the free and open generation and dissemination of knowledge. Known for its open and collaborative nature, the US research enterprise provides the foundation for a diverse and driven workforce, fostering discovery and innovation. International collaboration is crucial to scientific advancement and the success of research institutions in the United States.

  American universities have become a magnet for students and researchers worldwide to join forces in solving our nation's most pressing problems and promoting scientific advancement. Unfortunately, we are not playing on a level playing field. Our technological leadership is under siege from countries like Russia, China, Iran, and others whose rules for information

sharing and research integrity differ from ours. These countries are extracting intellectual capital, cutting-edge data, and technical expertise at an unprecedented rate and putting our technological leadership at risk. Academic sector entities must work closely with our federal partners to protect information and research with national security implications. To be most effective, integration and information sharing between the research security community and the U.S. counterintelligence enterprise must be seamless.

- **What can be done to enhance U.S. government agencies' ability to conduct investigations into grant fraud and technology transfer in collaboration with universities?**

  Robust relationships with our Federal partners and open exchange of information have been critical to our efforts to ensure the integrity and security of Federal grant funding awarded to Texas A&M System entities. When we learn of issues affecting our grant awards, we quickly report them to the appropriate Federal entity and take seriously any issues highlighted for us by our Federal partners.

- **To what extent should the State Department vet international students, professors, or employees from a counterintelligence perspective?**

  Understanding our collaborators is one of the most important aspects of any research security program. The Texas A&M University System's Research Security Office has established a robust open-source due diligence program through which we review all visiting scholars and post-doctoral researchers from countries of concern, all personnel engaging in our work with Army Futures Command, the University Consortium for Applied Hypersonics, and our national laboratory efforts, and others based on risk.

  Additional support, in the form of open-source information sharing or vetting information, from the Federal government would be welcome.

- **Should academic institutions do their research security vetting of visiting students, professors, and employees?**

  - **What tools, resources, and support from the IC would be needed?**

  As noted above, The Texas A&M University System's Research Security Office has established a robust open-source due diligence program, which we believe should be a model for academia. Institutions that cannot develop a research security/due diligence program like the A&M System would benefit from a federally funded regional due diligence program launched in partnership with an academic institution through which universities could seek assistance.

  We have developed several tools that allow us to scour open-source information more efficiently and effectively as part of our due diligence efforts. These tools have significantly decreased the time and staffing required to perform adequate due diligence. With minimal funding, these tools could be further developed and provided to other institutions to enhance due diligence capabilities.

- **How can the U.S. government, in general, and the Intelligence Community, in particular, better communicate the foreign intelligence threat to the American public, private sector companies, and academic institutions?**

To effectively communicate the foreign intelligence threat, the U.S. government, generally, and Intelligence Community, in particular, must work to understand the U.S. research enterprise and form partnerships with academic institutions. One cannot simply strike and replace industry for academia in bulletins and messaging – they are not the same. Messages must be tailored to the audience to have the most significant effect.

The ability to share actionable open-source information is also critical. While classified intelligence has its place, universities generally need access to UNCLASSIFIED, open-source information for their research security efforts. This allows for the broadest dissemination of threat information.

Clear communication channels between universities and their federal partners are also critical. The Texas A&M University System's Research Security Office is the single point of contact with Federal partners to exchange information related to threats from malign foreign actors. The RSO is a trusted member of the A&M research community and is in the best position to share relevant threat information with faculty and staff.

- **How can the U.S. government in general and the Intelligence Community in particular partner with non-Intelligence Community entities to prevent foreign intelligence penetration and exploitation?**

Key to our engagement with our federal partners has been the establishment of the Academic Security and Counter Exploitation (ASCE) working group, an association of university research professionals and their federal counterparts, which exists to leverage the expertise of universities that have demonstrated excellence in research security programs to help address the threat foreign adversaries pose to U.S. academic institutions.

The ASCE Executive Committee includes representatives from the FBI, DOD, State Department, and Commerce Department and meets bi-weekly to discuss threats to research security and mechanisms to combat them. The group works collaboratively to develop and share information on best practices for a successful research security program. ASCE also distributes a weekly Open-Source Media Summary to more than 3000 individuals from more than 300 academic institutions, government agencies, and cleared industries with ties to academia. Finally, ASCE hosts a four-day training seminar annually focused on securing the research enterprise. Now in its seventh year, the ASCE Seminar draws over 500 participants from academia, government, and industry each year.

- **Texas A&M has one of the most well-respected research security programs in academia.**

  - **What is unique about this program?**

First, the level of support we receive from the highest levels of the A&M System is exceptional. Chancellor John Sharp has stated publicly, "No one in higher education takes security as seriously as we do at The Texas A&M University System…and [we make] counterintelligence a priority, we intend to be a leader in protecting national interests and the sensitive work the Texas A&M System does in service to our country." With that kind of support from the top, it is easy to develop an exceptional research security program that is well-respected within academia.

Secondly, we have organized for success. We created a Research Security Office in 2016 and tasked it with oversight of the research security efforts for the 11 universities and eight state agencies that comprise the A&M System. A Chief Research Security Officer at the associate vice-chancellor level leads that office. The Chief Research Security Officer has extensive government and academic experience and holds a Ph.D. and credentials in industrial security.

The research security office oversees our classified research programs, our controlled unclassified information management, and our export control program. Our ability to manage these three overlapping programs from a single office provides excellent synergy and enhances effectiveness. The research security office has also developed an effective working relationship with compliance offices across the A&M System to provide unity of command and unity of effort in our mission to secure our research enterprise.

Texas A&M University System Policy designates the Chief Research Security Officer as the A&M System's single point of contact with federal partners engaging the A&M System on research security matters. This policy has resulted in more effective communication between the A&M System, its members, and our federal partners.

Thirdly, the A&M System developed a secure computing enclave in 2016 that allows us to secure federally funded research outside the wider A&M System networks. This secure computing enclave meets all the requisite NIST 800-171 requirements for protecting federal information on non-federal systems. We are also deploying a secure Microsoft® Government Cloud environment in which most of our large federally-funded programs will operate in the future.

Finally, we have chosen to take a leadership role in the national effort to secure our research enterprise. We established the Academic Security and Counter-Exploitation Program in 2017 to collaborate with other universities on this effort. The group has now grown to over 200 participating universities. We have published a weekly Open-Source Media Summary (OSMS) distributed to the academic community and our federal partners weekly at no cost. The OSMS provides timely threat information explicitly focused on the academic community. We also host an annual training that brings the academic community and its federal partners together to benchmark, share information, network, and move the effort for securing our research enterprise forward.

In short, the A&M System's research security program is unique because we have exceptional buy-in and leadership from the top down. We chose to act early, implementing the first research security office and establishing the first Chief Research Security Officer position in

academia. The A&M System implemented the requirements for NSPM-33 in 2016. Our program is also unique because we saw the need and chose to lead the research security effort in academia more than five years ago. We remain committed to that effort today.

- **How does Texas A&M assess the return on investment from its research security program?**

It isn't easy to put a price on our national security. We choose not to measure our research security investments in terms of profits and losses. The ultimate measure is how effectively we protect the federal research dollars we have been entrusted with and how our research contributes to the overall national-security effort. With that said, our research security effort has been designed for efficiency and effectiveness. The fact that our research security efforts have been recognized on a national level four times over the last six years by the Defense Counterintelligence and Security Agency suggests that our investments are paying high dividends in our ability to secure the research enterprise and contribute to our national defense.

- **To what extent has Texas A&M shared lessons learned with other academic institutions?**

As noted previously, the A&M System established the Academic Security and Counter Exploitation Program as a mechanism to leverage the expertise of universities with demonstrated excellence in research security programs to help address the threat that malign foreign actors pose to U.S. academic institutions.

We established the first Academic Security and Counter Exploitation Training Seminar in 2015 to provide a forum for those academic institutions participating in the NISP to benchmark and share best practices from their respective programs. The conference has grown since that first year to include the broader academic community and increased federal engagement from the FBI, DOJ, DOD, NSF, NIH, Office of the Director of National Intelligence, and Office of Science and Technology Policy. We were honored to have Chairman Warner and Senator Cornyn join the conference in 2021 to talk about the threat and the work you're doing here in Congress. We're well on our way in planning for next year's conference, which will be held in College Station from March 6-10, 2023. This year's seminar will have an international component for the first time resulting from our partnership with the Department of State.

While the Academic Security and Counter Exploitation Training Seminar provides an opportunity for academic security professionals to come together physically once a year, we have also developed ongoing platforms for virtual collaboration. We created a listserv for security professionals in academia to seek advice, benchmark, and share best practices daily. The listserv currently has over 200 member universities and 3000 individual participants and remains highly active.

We also share a weekly ASCE Open-Source Media Summary to share information with academia. We are pleased to reach over 3000 readers each week across academia, the private sector, and the Federal government, including from Capitol Hill.

- **Can you explain how university participation in efforts such as the Academic Security Conference helps those universities with less experience in research security address foreign influence threats such as foreign government-sponsored talent recruitment programs?**

As noted above, ASCE serves as a mechanism for universities, regardless of their level of research security experience, to collaborate and share information – both in person annually and virtually as often as desired – on threats they are seeing and best practices to address them.

The OSMS provides weekly actionable information on threats to the academic research enterprise directly to those individuals within the academic community who can address the threats. The OSMS also provides our federal partners with insight into the academic community's unique aspects so that they can better communicate the danger.

The annual ASCE Seminar provides an opportunity for academic security professionals to come together physically once a year with federal law enforcement agencies, research security policymakers, and leaders from government and academia to learn techniques for securing the research enterprise, benchmark, network, and collaborate.

- **What trends have you observed in the types of university research targeted by foreign governments in recent years?**

My observations tell me our adversaries cast a wide net in their efforts to access our technology. The focus is not solely on sensitive or proprietary research and technology. They are after fundamental research to facilitate their ability to leapfrog in the research process. Consequently, our efforts should have a wide aperture as well.

One very positive trend I see daily is the academy's progress in understanding, accepting, and addressing the research security threat over the past five years. The danger facing university professors, students, and institutions from malign foreign actors and foreign intelligence is widely understood and accepted today. Still, work remains to improve security and transparency across the research enterprise to allow us to continue operating in an open and collaborative environment on the international stage.