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

"Protecting American Innovation: Industry, Academia, and the National Counterintelligence and Security Center"

U.S. Senate Select Committee on Intelligence

Wednesday, September 21, 2022

About The Texas A&M University System

Chairman Warner, Vice Chairman Rubio, Senator Cornyn, and Members of the Committee thank you for the opportunity to testify before you today.

I come before you this afternoon as the Associate Vice Chancellor and Chief Research Security Officer 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 is one of the most extensive systems of higher education in the Nation, with an annual budget of $7.2 billion. Through a statewide network of 11 universities and eight state agencies, the Texas A&M System educates more than 152,000 students. It makes more than 24 million additional educational contacts each year through service and outreach programs. System-wide research and development expenditures exceed $1 billion and are drivers of our state's economy.

The A&M System has been a member of the National Industrial Security Program (NISP) since 1974. As a NISP participant, the A&M System is a cleared defense contractor just like Lockheed Martin, General Dynamics, or the more than 12,000 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.

The A&M System's security program has amassed a record of seven straight SUPERIOR ratings during annual Security Vulnerability Assessments conducted by the Defense Counterintelligence and Security Agency (DCSA). DCSA recognized the A&M System in 2015 and 2020 with the Colonel James S. Cogswell Outstanding Industrial Security Achievement Award as one of 40 from more than 12,000 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. DCSA also recognized the A&M System with their 2017 and 2019 Awards for Excellence in Counterintelligence, given to those contractors and universities that best demonstrate the ability to stop foreign theft of US defense and national security technology.

Addressing the Threat

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.

Acknowledging this risk, A&M System Chancellor John Sharp established the Research Security Office (RSO) at the System level in 2016 to provide program management and oversight of all classified research, controlled unclassified programs, and export-controlled research across the 19 A&M System members. The RSO manages the A&M System's relationship with DCSA 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 visit 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.

Understanding our collaborators is one of the most important aspects of any research security program. With whom are we collaborating? Who is funding those collaborators? Is there a foreign government nexus? What is the risk to the institution? Is there a reputational risk? Can these risks be mitigated? To answer these questions, the RSO 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.

We require the mandatory disclosure of all foreign collaborations and approval of foreign travel. We conduct continuous network monitoring and have included keywords and signatures in our data loss prevention system explicitly focused on identifying malign foreign influence in our research enterprise. We have updated our conflict of interest and conflict of commitment policies and have established processes for reviewing and approving foreign collaborations and agreements.

We have established a NIST-800-171 compliant secure computing enclave that is available to all members of the A&M System to protect sensitive research funded by the federal government. The secure computing enclave allows us to monitor the flow of information down to the project level. It precludes anyone who might achieve unauthorized access to our secure computing enclave from gaining access to more than a single research effort.

Underpinning all this work is our robust relationship with our federal partners, including the Federal Bureau of Investigation (FBI), DCSA, Department of Justice, and other members of the Intelligence Community. FBI Director Wray noted, "we can't arrest our way out of this problem." Collaborations between academia and the Federal government are critical to addressing these threats. The RSO serves as the single point of contact for the A&M System with our Federal partners. I engage with our FBI and DCSA partners daily to facilitate information sharing and joint operations.

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.

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 remains extremely active. We also established the Academic Counter Exploitation (ACE) Program as a secure portal on the DHS's Homeland Security Information Network to allow academic institutions to share threat information unique to academia. We also share a weekly ASCE Open-Source Media Summary as another mechanism 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.

Recommendations

Academia has come a long way 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 the state of security and transparency across the research enterprise to allow us to continue to operate in an open and collaborative environment on the international stage. National Security Presidential Memorandum-33 (NSPM-33) will help in these efforts by setting forth the actions required by research institutions, including academia, to mitigate risks and enhance the protection of the US research enterprise.

Universities seeking to implement effective research security programs should consider an approach that puts several organizational, process, policy, training, and technology solutions in place. These solutions should focus on mitigating the risks to the research enterprise while protecting those characteristics that make the US higher education system the most productive and prolific worldwide research generator. The institution should integrate research security functions into every level of the organization. Institutional leaders should champion research security and integrity as integral to the overall success of the research enterprise.

Implementing an effective research security program can significantly enhance the security of an institution's facilities and intellectual capital. Research personnel must be aware of existing risks, be able to implement countermeasures when appropriate, and be observant of nontraditional collection activities directed at their institution to be effective. This outcome is possible only if all institution members know the range of threats to the research enterprise and actively support the risk assessment and management program.

Research security countermeasures take several forms, including process solutions, policy solutions, and technology solutions. Process solutions include vetting visiting scholars, monitoring computer networks for illicit exfiltration of data, incorporating data-loss prevention systems, and establishing robust risk-management and risk reporting frameworks. The RSO should integrate processes for securing the research enterprise into every aspect of university operations, including human resources, awareness and training, information technology, international travel, and business administration.

Conflict of commitment, financial conflict of interest, external employment, and international travel policies have important research security implications. Establishing clear, enforceable expectations in these areas through well-thought-out organizational policy is critical to an effective risk- management program.

Incorporating technical solutions, such as secure computing enclaves that meet federal requirements for information protection, into risk-management processes can provide a solid foundation for securing data while minimizing the burden on researchers. We were pleased to see the inclusion of a regional secure computing enclave pilot program in the CHIPS and Science Act (P.L. 117-80). This pilot would assist universities conducting federally funded research in meeting security requirements, such as NIST-800-171. The requirement to meet this standard exists regardless of the size of the university or the size of the research award. Yet, compliance can be costly. The regional enclaves authorized in this bill would provide a secure network on which universities of all sizes could store their sensitive research. It would help universities better monitor traffic on their systems and enhance the protection of federally funded research from foreign theft. We look forward to working with the National Science Foundation as they implement this provision.

Just as there is a disparity between larger research institutions and smaller regional universities in their ability to protect sensitive information effectively, the capabilities of academic institutions to conduct effective due diligence in vetting visiting scholars vary widely. This is another area where the research security community could benefit significantly from sharing resources. Larger research institutions could serve as regional hubs that smaller universities could rely on for assistance and resources in vetting visiting scholars. These regional hubs would serve as clearinghouses for federal-level coordination with the counterintelligence community.

Finally, there is a need for a National Center of Excellence (COE) for Research Security within the academic community. This COE could be a focal point for developing awareness and training material tailored to academia. It could provide training to research security offices on practical techniques for vetting visiting scholars, among other topics. It could also offer advice and assistance to universities in establishing and maintaining effective research security programs. This National Center of Excellence for Research Security could build upon the work that groups like the Academic Security & Counter Exploitation Program have already begun.

Conclusion

The excellence of the US research enterprise is inseparable from its commitments to openness and academic independence, institutional autonomy, and discretion to operate in a globalized world. However, these qualities also engender vulnerabilities to national and economic security in a climate of sharpening strategic competition. Rest assured, our adversaries will not rest on their laurels and will attempt to adapt to our efforts. We in academia must remain vigilant to meet the threat and protect the intellectual property that makes our nation the most prosperous in the world.

While the most effective way to address this challenge is for the academic community to take the lead in establishing policies, procedures, and protocols to secure the research enterprise, this is not a fight we can win on our own. The U.S. Government, including NCSC and other members of the Intelligence Community, play critical roles in notifying, supporting, or defending academic entities from foreign intelligence attack, penetration, and manipulation. Our collective success is dependent upon the effective partnership working toward common goals. The Texas A&M University System takes these threats seriously and looks forward to working with you and our partners in the Federal interagency, academia, and the private sector to address them.