Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the Academic Security and Counter Exploitation Program's Seventh Annual Seminar

March 8, 2023

Good afternoon. Thank you, Dr. Gamache, for that generous introduction and for the invitation to join you today. And thank you for your leadership – and the leadership of Texas A&M – on academic security and counterexploitation issues. You heard from Assistant Director Alan Kohler yesterday about what the FBI is doing to promote academic security. Today, I want to talk to you about what we at the Department of Commerce's Bureau of Industry and Security, or BIS, are doing to help you protect both your research and the open collaborative environment that drives it.

But first, I want to talk about the 12th Man. Last year, Texas A&M celebrated 100 years of the 12th Man tradition. For those unfamiliar with it, that's the tradition where the fans at Aggie football home games spend the entire time on their feet, hooting and hollering, thereby becoming a metaphorical 12th player on the field. It all arose out of something that happened way back in 1922. The Aggies were facing the top-ranked and undefeated Centre College Praying Colonels. Yes, you heard me correctly, the Praying Colonels. And, yes, you also heard correctly, Centre College, which now plays in Division III, was the number one college football team in the country. Anyway, the Aggies were worried about having enough players to finish the game – they were shorthanded and kept losing more men to injury.

A Texas A&M basketball player by the name of E. King Gill was in the stands watching. As the Aggies coach took stock of his rapidly thinning bench, he saw Gill in the stands and called him down. Gill ran under the bleachers and put on the uniform of an injured running back. Gill stood ready to play throughout the game, becoming "the 12th Man" in what was one of the greatest upsets in college football history, with the Aggies winning 22-14. In the end, Gill didn't enter the game. But he was dressed and ready, just in case he was called on to play.

This Aggie tradition of the 12th Man is now a protected one. It's true. The university trademarked the term with the U.S. Patent and Trademark Office, which is part of the Commerce Department, where I work. When the Seattle Seahawks, started using the phrase to describe their home fans in the early 2000s, A&M sued them in court. The case settled and the Seahawks now pay the university to use the term.

In other words, when it comes to the 12th Man, Texas A&M worked with the Commerce Department to successfully protect their idea from misuse by others. It's that type of collaboration between academia and the Commerce Department – a partnership that protects innovation from misuse – that I want to speak with you about today.

* * *

Texas A&M is a research and development powerhouse. Among other achievements, it is a collaborator on large-scale engineering projects such as the Giant Magellan Telescope in Chile. This telescope, which will be the most powerful on earth, will be able to produce unprecedented images of our galaxy. Twelve stories tall, with seven primary mirrors, the telescope will be used to study the first galaxies that ever formed and search for life in the atmospheres of potentially habitable planets. Some of the state-of-the-art optics systems that will be used in this telescope, including first-light instruments, are being built right here at Texas A&M.

But Texas A&M isn't doing this work alone. The Giant Magellan Telescope is being developed by an international consortium of 13 leading research institutions. Both U.S. universities like A&M, the University of Chicago, and Harvard, and research institutions abroad, like the Australian National University, the Sao Paolo Research Foundation, and the Weizmann Institute of Science in Israel. The mind-boggling research that will be done once the telescope is completed later this decade will only be possible because of this collaboration, not only across disciplines but across institutions and across countries.

Our research institutions are strongest and most productive when they collaborate with partners, including international ones. But at the same time, our open, collaborative research environment, which is the hallmark of American academia and one of its greatest sources of strength, also presents an inviting target for foreign adversaries who wish to exploit that environment and misappropriate our research. In an age where you can share even the most sensitive and valuable research in an e-mail, over Zoom, or through visual inspection of certain manufacturing schematics, our research universities must be relentless in their efforts to protect themselves.

We're here to help. As the Assistant Secretary for Export Enforcement, I oversee a team of law enforcement agents and analysts focused on a singularly important mission: keeping our country's most sensitive technologies out of the world's most dangerous hands. One of our most important partners in this endeavor is academia.

Last summer, we established a comprehensive effort – our "Academic Outreach Initiative" – to help academic institutions maintain their open, collaborative research environment in a way that also protects them from national security risk. Through this initiative, we have strategically prioritized our engagement with universities whose work gives them an elevated risk profile.

When we rolled out the Initiative, we identified twenty research institutions that either possess ties to foreign universities on the Entity List; host a strategic Department of Defense University Affiliated Research Center, also known as a UARC; or conduct research in sensitive technologies subject to the Export Administration Regulations.

All twenty agreed to partner with us. We're now working on identifying additional universities who meet one or more of these criteria, but who were not part of the initial group of twenty. We'll be reaching out to them in the near future about joining the Initiative. And if there's an institution that meets one of the criteria and wants to reach out to us to join, we welcome that too.

Each of the twenty institutions has been assigned a dedicated "Outreach Agent," a specific agent from their local BIS office who meets with them quarterly and serves as a resource and point of contact. Over the past few months, we've also presented two different webinars to our partner institutions. The first focused on how export controls apply in academic settings and on ways to identify the national security threats facing universities. The second was a training on how best to conduct open-source research to better vet potential foreign partners. This spring, we'll be offering a broader training on regulatory requirements, including fundamental research in academic settings.

Separate from our Academic Research Initiative, we recently launched a Disruptive Technology Strike Force with the Department of Justice, the FBI, and Homeland Security. The Strike Force's goal is to protect critical technological assets from being acquired by nation-state adversaries. The types of technologies that the Strike Force will focus on are ones where our research universities are playing a critical developmental role, including advanced semiconductors, supercomputing, quantum computing, hypersonics, and biosciences related to enhancing human performance like brain control interfaces.

The Strike Force will focus enforcement resources in locations across the country to protect cutting-edge research from misappropriation. In short, through both the Academic Outreach Initiative and the Disruptive Technology Strike Force, we're committed to doing all that we can to both protect national security and maintain U.S. leadership in academic research and innovation.

* * *

The challenge faced by research institutions of how best to safeguard their research is not just an American challenge. It's an international one. Allied countries with world-renowned research universities face the same quandary as American ones – how to protect sensitive research from theft and diversion by nation-state adversaries while maintaining an open research environment that encourages the free exchange of ideas. And just as we at the FBI and BIS are working through that quandary with American institutions, several allied governments are doing the same in their countries.

Take the United Kingdom. There, the government published guidance on how UK export controls apply to academic research and what academics should watch out for as they conduct research with overseas partners. As noted in their Higher Education Export Control Guide and Toolkit, awareness of and guidance on export controls should form an integral part of an academic institution's research policies.

Similarly, the Australian government, in collaboration with their academic community, published the Guidelines to Counter Foreign Interference in the Australian University Sector, which were updated in 2021. The guidelines seek to safeguard the security of Australia's university sector without undermining its invaluable openness. The guidelines delineate four foundational elements for building resilience within a university: (1) governance and risk mitigation; (2) communication, training, and information sharing; (3) regular due diligence and risk assessments; and (4) cybersecurity. Like we do in our Academic Outreach Initiative, the Australian government is working in partnership with Australian universities to share information and raise awareness about the importance of protecting academic research.

In January, I met with counterparts in Canada to discuss, among other things, their approach to academic research security. The Canadian government has launched a "Safeguarding Your Research" portal, which provides information to the Canadian research community on how to safeguard their research and innovations. Canada also publishes a "Protect Your Research" guide, which is broken down by geographic region to reflect the nuances of each province and territory – highlighting specific industrial sectors, research institutions, and technology hubs in each place. Additionally, in 2021, the Canadian government released its National Security Guidelines for Research Partnerships, which integrate national security considerations into the development, evaluation, and funding of research partnerships. As I stated during my visit to Ottawa, we're committed to working closely with our Canadian counterparts in helping academic institutions in both countries protect themselves from current and future threat actors.

* * *

One aspect of university research that we and allied countries are thinking about is fundamental research. Scientific and technological breakthroughs are only possible because of foundational research that precedes those breakthroughs. Experimental and theoretical work must be shared, tested, and peer-reviewed. In the case of dual-use technology, the UK calls this "basic scientific research," which is undertaken solely to obtain new knowledge of the fundamental principles of phenomena or observable facts. It is not directed towards a specific practical aim or goal.

Here, the term "fundamental research" refers to scientific and technical research that is intended for publication and widespread dissemination within the academic community. As long as researchers do not accept restrictions on publication for proprietary or national security reasons, the results of fundamental research are generally not subject to the Export Administration Regulations, or EAR. Therefore, sharing technology or software that arises during, or results from, this research will likely not require a BIS export license.

Note that I just said, "will likely not require a BIS export license." The key word is "likely." There is sometimes a misconception among professors that any research destined to be published is wholly exempt from export controls because it qualifies as fundamental research. While this is true as a general matter, there are some important exceptions that I want everyone to be aware of. I'll touch on just two of those exceptions here – government-funded research and changes during the research cycle.

First, it is important to note that technology and software that is produced through a U.S. Government-funded research project might not be considered "fundamental research" if it is protected by government-imposed access and dissemination or other specific national security controls. These national security controls include prepublication review requirements, restrictions on publication or dissemination to non-U.S. citizens, or the restriction of participation in the project to U.S. citizens only.

And second, remember that just because your project falls within the definition of fundamental research at the outset, it does not mean that it will in the middle, or at the end, as publication decisions may shift. As an example, take a project where at the beginning everyone intends that the research will be published without restrictions. The project is therefore considered fundamental research. But then, mid-project, someone sees a unique commercial use for the technology and decides that it is now proprietary information and will instead be protected. If that happens, it would no longer be considered fundamental research, would become subject to the EAR, and may require a BIS license. For this reason, an assessment should be made at every stage or development of a research project.

In summary, even if you are conducting fundamental research, you still may be required to obtain a license if your activities fall under one of the exceptions. The question of compliance does not just end once you determine that what you're producing is considered fundamental research.

Instead, it comes down to the facts. Each university research program is different. Each individual research project is different. The final determinations on fundamental research are fact specific. If you need assistance with this determination in your individual case, please reach out to your compliance team, your export control officer, and/or the BIS Office of Exporter Services. You can also choose to file an Advisory Opinion request. We have a lot of resources at your disposal so please don't hesitate to contact us.

* * *

Export controls are not static. And they play an increasingly important role on the global stage. Just reflect back on the past year: export controls and sanctions have been some of key tools that the United States has used to respond to Russia's unjustified and brutal war against Ukraine. We've built a coalition with 38 other countries to put in place the most expansive export controls in history aimed at a specific country. As a result of those actions, the Russian military has turned to pariah states, like Iran and North Korea, to replenish its supplies with inferior and defective equipment.

As the nature and scope of export controls change, it is incumbent on everyone to take notice. If I can impart three pieces of advice to those who work in academia, it would be this:

First, export controls should be everybody's concern, not just something your compliance team thinks about. You – and I mean everyone at a university, including professors, research assistants, students, counsel, academic deans, etc. – should be thinking about how export controls fit into your roles and responsibilities.

You don't need to be an expert on the EAR, but you do need to know how to spot red flags and when to reach out to your export control officer for further guidance.

Checking in with the export control officer could have prevented one Ivy League university from exporting various strains of animal pathogens without the required license to overseas research institutions in Canada, Belgium, France, and other countries. The items fell under chemical and biological weapons export controls that exist to keep the building blocks for these weapons out of the wrong hands. University staff only realized their error during a subsequent training session on export controls. This type of unforced error – one that could have been avoided with a call to the right people at the outset – underscores how important it is that everyone think about how export controls may relate to your research and have procedures in place to guide your staff.

Second, you should always do a risk assessment before collaborating with international partners. We recommend vetting any potential partner in at least two different ways: (1) through an open-source search, for example by using a search engine like Google, to see what is in the public domain; and (2) checking the name of your potential partner against the Consolidated Screening List, which is a free online tool administered by the Commerce Department. If you see any news articles, press releases, or NGO publications that link your potential partner to foreign military or defense projects, foreign intelligence or security services, or other end-users of concern, you should reach out to your compliance team, your export control officer, or BIS. As I said earlier, international collaboration is an essential part of academia. The Giant Magellan Telescope, for example, is a good illustration of the importance of working with partners across the world. Without strong international partnerships, we wouldn't be close to unlocking the secrets of the universe. But without strong internal controls, you could end up partnering with institutions that serve the interests of hostile foreign governments as well as the interests of scientific discovery.

Third, as the Canadians say, "Protect your Research." From a prudential standpoint, think about the purpose of your research and the motivations of your partners. You don't want to risk your reputation by inadvertently partnering with someone who has nefarious intentions. And that's true regardless of whether you're engaged in fundamental research or not. We want you to have confidence in your collaborations and to make informed decisions concerning all of your research. If you have offers from foreign entities to purchase or invest in your research that seem too good to be true, listen to your gut and call your compliance team, your export control officer, or us at BIS.

* * *

In reflecting back on becoming the legendary 12th Man, E. King Gill once told a reporter, "I wish I could say that I went in and ran for the winning touchdown, but I did not. I simply stood by in case my team needed me."

Gill's willingness to serve is reflected throughout the history of Texas A&M, well beyond the football field. Aggies have played key roles in our government, military, and civil society. By 1918, almost half of Texas A&M's graduates were serving our country in World War 1.

During the Second World War, over 20,000 Aggies contributed to the war effort, which resulted in seven Aggies receiving the Medal of Honor. Thousands of additional A&M graduates have continued to serve their country since then.

When it comes to protecting our country's sensitive technology from foreign adversaries, we need everyone to step up and serve. Compliance with export controls must be a team effort. As the Australian guidelines on countering foreign interference note, "[s]ecurity is a collective responsibility with individual accountability." Whether you're an export control officer or the Vice Provost for Research, a professor or a research assistant – your efforts are critical to protecting that innovative and groundbreaking research for which our U.S. research institutions are rightly famous. Our shared mission is to protect that research and to prevent it from falling into the hands of those who would do our country harm.

Thank you.

####