FOR IMMEDIATE RELEASE
May 5, 2022
www.bis.doc.gov

BUREAU OF INDUSTRY AND SECURITY
Office of Congressional and Public Affairs
OCPA@bis.doc.gov

KEYNOTE ADDRESS TO
ASSOCIATION OF UNIVERSITY EXPORT CONTROL OFFICERS
2022 CONFERENCE ON EXPORT CONTROLS AND RESEARCH SECURITY AT HIGHER EDUCATION AND SCIENTIFIC INSTITUTIONS
ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION
THEA D. ROZMAN KENDLER

Delivered May 4, 2022

Remarks as Prepared for Delivery

Thank you for the opportunity to speak with you today. As a Penn Law school alumna, I'm honored to be delivering these remarks here at Penn, although it is a little surreal to be up here on the stage with Dean Ruger.

Places like Penn and the institutions the export control officers of AUECO represent shape new generations of entrepreneurs, scientists, engineers, teachers, and yes, lawyers. I am thrilled to partner with you all to educate all these stakeholders on the importance of export controls.

While the U.S. higher education system is the crown jewel of our open society, it is also a front line in protecting our national security.

We face real threats to the principles of rule of law and democracy around the world. And we strive to ensure that U.S. innovation does not benefit adversaries who seek to undermine those values.

Consider the ongoing, brutal Russian assault on Ukraine. Underlying that senseless war is Vladimir Putin's warped sense of grievance against Ukraine and disregard for the free, open, rules-based order.

Also consider Xi Jinping's rejection of democratic values and human rights, not just in Xinjiang and Tibet, but across China's population, not to mention its military-civil fusion strategy and military expansion across the region. Our strategic competition with the People's Republic of China is one of the defining challenges of our time.

We reject the notion that going the way of state-run kleptocracy and ethno-nationalism based on repression and human rights abuses is a viable path for any nation to take. Our challenge is to demonstrate that our principles of tolerance, respect for human rights, and the rule of law, are the

surest paths to long-term prosperity for every nation. That challenge has only gotten bigger in recent years as commercial technologies have become more sophisticated.

The phones that we have in our pockets are tremendously powerful tools. They can take amazing pictures of our family—or become tools of surveillance and repression.

We are seeing this link between commercial technologies and national security play out in Ukraine, where semiconductors produced by Western firms have turned up in Russian military drones and other applications.

More and more, this link between commercial technology and national security requires us to think about how technological breakthroughs and innovation will operate outside the lab, in the worst-case scenario.

You may be aware of the criminal case against Xu Yanjun in Ohio – he was a Chinese intelligence officer tasked with obtaining jet engine technology from a U.S. company. Or the case against Mozaffar Khazaee in Connecticut – while working for U.S. defense contractors, Khazaee obtained controlled U.S. technology, which he sought to take to Iran, in part to aid him in finding work at an Iranian state-owned technical university.

It's true that industry and academia require different approaches to export controls, and the Xu and Khazaee cases are examples of technology that was held by private companies, not research institutions.

But these cases also show that when foreign countries cannot legally obtain U.S. technology, they will resort to whatever means necessary.

There is no distinction between industry and academia for a procurement agent.

Let me also draw your attention to the risks associated with collaboration with unvetted foreign institutions. We value, and we know that your faculty and researchers value, international collaboration. How would they feel, though, to know their science and engineering support a military program contrary to U.S. national security? Attacks on innocent civilians? A government mass surveillance program? Human rights abuses? For your faculty and researchers, these are not just national security, but also ethical concerns. And how about the reputational risk to your institutions of being associated with a program engaged in these activities?

The AUECO website poses the question, "Why do U.S. universities need to worry about export controls?" I respectfully suggest that the answer is not – or at least isn't solely – that unauthorized exports can result in fines and jail time.

Rather, universities should cooperate with export controls because export controls protect innovation and national security.

Controlling exports, of course, is not the same as cutting off exports. Export controls on a technology enable us to look at the destination, end use, and end user involved in a collaboration. This gives us insight into whether such exports or collaborators are a U.S. national security

concern. They help you and your faculty and researchers do the due diligence to protect you from exposure to the concerns I know we share.

Our job – yours and mine – is to make sure that American innovation is protected. Protected from use in shocking human rights abuses, military attacks on innocent civilians, and theft by those who seek to illicitly procure what they can't obtain within the bounds of the law, certainly without regard to intellectual property rights.

Even research that appears inherently civilian may have national security implications. And I am grateful to you for making your faculty and researchers aware of these concerns.

Why this is relevant to you, and the higher education system writ large, is that the academic community is a critical partner in our efforts.

I am here today to thank you for your help in this effort and to ask for deeper collaboration between us. A strong relationship between the Bureau of Industry and Security and the institutions you represent is essential to ensuring U.S. national security, including long-term technological leadership.

I would be shocked if you told me that your institution does not engage in international collaboration.

But we at BIS know that there is no one size fits all approach for academia. Some of your institutions focus only on fundamental research. Others operate classified labs working at the cutting edge of military technology. And many operate somewhere in between.

Different institutions have different needs and different challenges.

We are trying to better understand how we can help you support your institutions. We want to provide better resources and support, tailored to the issues that keep you – the compliance officers – up at night.

To this end, when BIS issued a survey to AUECO membership in 2020. We received great feedback from many of you all about how BIS can help. I'd like to hear from more of you, though. Given how different your institutions are, we want to know how we can address your different needs.

In fact, you can provide that feedback right after I'm done. As I know has already been mentioned by other BIS speakers this week, copies of BIS's survey are available at the registration desk. I'd ask you to please fill these out and return them to the same location. I will be reviewing the survey results to assess how we can better engage with academia. Thank you in advance for your participation in this information-gathering.

Let me also point you to the resources we have made available for you to use in your individual institutions.

The BIS website provides short videos on topics including deemed exports, how to classify items subject to the EAR, license exceptions, and reexports and offshore transactions. These videos

are designed to be short introductions on their topics and may be useful to you as you train your colleagues.

We also developed an academia-specific export controls brochure for you to share with your community members. I heard that the brochure was provided to some of you at an event last year. Thanks to AUECO and Penn, we are able to make it available to the rest of you through the link posted on the slide. Note that BIS designed this brochure for you, as ECOs, to provide to faculty and researchers who may be less knowledgeable about export controls. We welcome your feedback on how we can better tailor our message, starting with how our national security message can best resonate in your institutions.

Export Control Officers are indeed the front line in our export controls, and we want to support you as you protect our national security. Please help us understand your challenges, needs, and how we can best help.

Let me change gears for a minute and mention a concrete area where we seek your help and that of your faculty.

As you know, the Export Control Reform Act (ECRA) Congress enacted in 2018 specifically identified BIS's responsibilities for reviewing and controlling emerging and foundational technologies.

We were already doing this as part of our regular proposals for new controls to the multilateral regimes. ECRA gave this work a new boost, and BIS has strived since August 2018 to cast a wide net for emerging and foundational technologies that are not already identified in the Export Administration Regulations and ought to be.

I recognize that there is some controversy surrounding this area. Some claim BIS has not defined what emerging and foundational technologies are, has not acted fast enough, and hasn't been willing to act unilaterally. Others criticize the notion of controlling emerging technologies at all because such action will harm innovation.

Let me be clear. If a technology poses a risk to national security, BIS controls it.

That may be because of the inherent nature of the technology or because of the risk of it falling into the wrong hands. We are responsive to national security threats posted by new technologies and innovations of old technologies, whether or not we formally identified the technologies as "emerging" and "foundational."

Shortly after ECRA's enactment, we published a list of 14 general technology categories and invited comment on what types of items, applications, technologies pose a national security threat. For your reference, those areas are:

(1) Biotechnology;
(2) Artificial intelligence (AI) and machine learning technology;
(3) Position, Navigation, and Timing (PNT) technology;
(4) Microprocessor technology;

(5) Advanced computing technology;
(6) Data analytics technology;
(7) Quantum information and sensing technology;
(8) Logistics technology;
(9) Additive manufacturing;
(10) Robotics;
(11) Brain-computer interfaces;
(12) Hypersonics;
(13) Advanced Materials; and
(14) Advanced surveillance technologies.

Over the last 3½ years, we have imposed 38 new technology controls we identified as emerging or foundational under Section 1758 of ECRA.

All but one of these controls were established through multilateral regimes, meaning that U.S. exporters and their counterparts in other major economies of the world faced the same export controls.

We know from your industry counterparts that multilateral export controls help maintain a level playing field. In the academia context, this means collaboration with partner country institutions is easier.

I'd also note that in identifying emerging and foundational technologies, ECRA requires us to consider:

- The development of emerging and foundational technologies in foreign countries;
- The effect export controls may have on the development of such technologies in the United States; and
- The effectiveness of export controls on limiting the proliferation of emerging and foundational technologies in foreign countries of concern.

As you can see, our mandate under ECRA starts with national security, but also directs us to be thoughtful and to carefully tailor controls.

We must get this right. To do so requires technical understanding, including the benefits and concerns associated with specific technology. And it requires acting in a tailored, targeted way to protect national security while supporting American technological leadership.

I'd ask for your help with this effort.

Given the widespread threats we face, we can't have our academic institutions, researchers, and faculty stick their heads in the sand and reflexively hold that all controls are bad for innovation.

Carefully tailored export controls support innovation.

They encourage due diligence with respect to partnerships—That will help to protect intellectual property and ensure that partners with whom your faculty and researchers seek to collaborate won't divert research to dangerous ends.

Consider nuclear technology. We have a well-developed and understood regime for control of nuclear technologies. This helps to protect our national security—not to mention global security.

Yet, we still see nuclear technology innovation in energy and health care, among other civilian, commercial industries.

Certainly, not all our 14 identified emerging technology sectors will end up with the kind of robust, multilateral regulatory regime that nuclear technology has.

But the risk of failing to think through the national security concerns of new technologies is real. Developing technologies without considering how they may be applied outside the lab is reckless. Failure to consider the guardrails – based on national security, ethics, and values – that we need to establish during the development process can have serious consequences.

Let me share an example in the biotechnology field.

Biotechnology and life sciences are areas of amazing technology potential. But technology is value neutral. It's people who determine how that technology will be used and in what applications.

Last year BIS asked for public comments on a control we were considering on brain computer interface (BCI) technology.

We received 18 comments, the general thrust of which was: Don't regulate or you'll kill innovation.

The potential applications of BCI technology are many, and their impact could be profound.

Around the same time that we closed the comment period on our BCI notice, BIS added a series of parties to our Entity List for attempting to develop and deploy biotechnology and other technologies for military applications and human rights abuses.

We added the Chinese Academy of Military Medical Sciences (AMMS) and eleven of its research institutions to the Entity List, according to the Federal Register Notice:

> "…based on the body of information that AMMS and its eleven research institutes use biotechnology processes to support Chinese military end uses and end users, to include purported brain-control weaponry. This activity is contrary to U.S. national security and foreign policy interests . . ."

"Brain-control weaponry" sounds a lot different from BCI technology.

I understand the initial instinct behind the commenters' responses to our request for comments on BCI technology. But an outright condemnation of export controls is not tenable given the potential for the technology's nefarious uses.

Your faculty and researchers are likely focused on collaborating with the best minds in their fields. Are they thinking about who else is interested in the technology, and the worst-case scenarios? Export controls will help them do that.

We're on the precipice of tremendous technological advancement in many of the labs and research facilities you oversee, and we need your help.

I hope that I've illustrated that BIS's concerns are tangible and real, that the responsibility for protecting national security is shared, and that you are valued partners. I thank you for your critical role in raising awareness of export controls and doing your part to create a more secure and prosperous future.

You have an important job, and BIS wants to help you do it, because we will all benefit.

Before I close, let me share a personal observation with you.

I grew up in an academic community, the daughter of a professor whose career was based on international collaboration. My family lived overseas when my father had a sabbatical year at a Japanese university. I understand the value of global education and research. And I share the view that the openness of U.S. universities makes them second to none.

BIS is your partner, and my door is open to you and the specific issues facing your institution.

We have shared interests and responsibilities. Protecting national security. Supporting the next generation—of people, and of technologies.

Thank you.

###
