FOR IMMEDIATE RELEASE
October, 2022
www.bis.doc.gov

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

Remarks As Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod at Oregon State University on the Academic Outreach Initiative

October 26, 2022

Thank you, John, for the generous introduction. And thank you to Oregon State University for hosting us today.

It's great to be here in Oregon. Oregon was among the top 20 export states in the U.S. last year, with overall exports valued at $29.6 billion. Computer and electronic products have been Oregon's number one export for several decades now, representing almost 50% of the state total. Leading the way are semiconductors, which comes as no surprise with Intel located in Oregon's Silicon Forest. Interestingly, it was an Oregon State alum who played a vital role in the creation of Intel's 386 32-bit microprocessor, a key milestone in the history of semiconductors that revolutionized the personal computer industry.

The size of a fingernail, semiconductors contain billions of electrical switches and are critical to the functioning of nearly every piece of technology today—from the phones in our pockets, to the cars we drive, to advanced military applications. They are the quintessential dual-use commodity. They play a critical role in not only Boeing's commercial aerospace business but also its military one. Semiconductors power data-processing units used both by Nike and by the Umatilla Army Depot, for everything from payroll to inventory monitoring systems. And they're an essential component of the unmanned aerial vehicles that can help the Departments of Transportation in Oregon and Washington conduct

bridge inspections, but they also can be misused in kamikaze drones in Ukraine. It is the use – or rather – misuse of U.S. semiconductor and other advanced technologies by our adversaries to support military modernization and WMD programs that is our core focus at Export Enforcement.

* * *

Earlier this month, President Biden released the National Security Strategy, which describes the current national security threat environment and the Administration's vision on how best to address it. The Strategy is the culmination of years of hard work by hundreds of government employees across many different federal agencies. It provides a roadmap – or a syllabus, if you will – for how we will work to advance our vital interests and pursue a free, open, and secure world.

When the first National Security Strategy was presented to Congress by President Truman in 1950, the world was in recovery from two World Wars. The ideological clash at the time was communism versus capitalism, and our greatest geopolitical rival was the Soviet Union. Today's Strategy has some of the same parallels. The world is in recovery from a global pandemic. We're defending democratic values against the encroachment of authoritarianism, and our most pressing strategic challenges are China – which happens to be the number one export market for Oregon – and Russia.

As the Strategy makes clear, our two greatest priorities are out-competing China and constraining Russia. So-called "traditional" national security threats – like WMDs, arms control, and terrorism -- remain pressing, but have been overtaken by the even more urgent ones from China and Russia. Confronting the challenges posed by nation-state actors like these cannot be met by military might alone. We must also shape the rules that govern the development of technology, cybersecurity, trade, and economics.

What this means, at a practical level, is that the domain of national security and the domain of academia are growing increasingly interconnected. Our country's technological leadership and our economic dynamism stem from the strength of our academic institutions. Advances in fields like artificial intelligence (AI), biotechnologies, robotics and automation, and smart materials will play a critical role in advancing our national security interests over the next decade. Oregon State and the University of Washington, for example, are doing cutting-edge work on nanotechnology infrastructure. Stanford is conducting pioneering research in all areas of AI, including on robotics and machine learning. University

research will continue to drive big breakthroughs in a variety of scientific and technological fields.

These breakthroughs will be important for academia. But they'll also be critical on the national security front. The experts assess that, eventually, quantum computers will be so powerful that they will enable unbreakable encryption. And, that their computing power will allow whichever country develops the technology first to break all existing encryption. Whichever researcher develops that technology first will be a strong candidate to win the Nobel prize. But whichever country develops that technology first will be a strong candidate to be the world's dominant superpower. And that's just one technology. Others, like AI, biotechnologies and hypersonics are similarly capable of providing military overmatch to the country that develops them first.

As Jake Sullivan, the National Security Advisor, recently put it, we need to lead in the areas of these "force multipliers." Maintaining a "relative advantage" no longer cuts it. The sliding scale approach of staying only a couple of generations ahead is untenable in the long run. Instead, we need to maintain as large of a lead as possible. And to do so, we need to protect our technology advantages and prevent our adversaries from using our technologies against us or their own people.

* * *

Our work at Export Enforcement reflects this growing convergence between science and technology, on the one hand, and national security on the other. In a world where even the most sensitive and valuable research can be exported in an e-mail exchange, our research universities unfortunately present inviting and potentially vulnerable targets. According to public reporting, in 2019, hackers associated with the Chinese government targeted universities in the United States to steal research on undersea technology. And the Cybersecurity and Infrastructure Security Agency, or CISA, recently published a joint cybersecurity advisory with the FBI and the NSA about the new techniques that the PRC uses to conduct malicious cyber activities. These techniques – which include stealing IP and accessing sensitive networks – are used, and will continue to be used, against a wide variety of sectors, including academia.

If our adversaries can't steal your research through the back door, they may attempt to do so through the front door – by taking advantage of partnerships with academia. Take iFlyTek, a well-known partially state-owned Chinese technology

company that specializes in artificial intelligence and voice recognition software. In 2017, Human Rights Watch publicized the relationship between iFlyTek and the Xinjiang police, who were using the software to develop a pilot surveillance system to identify and monitor Uyghurs. Despite that public reporting, just one year later, in 2018, iFlyTek announced a five-year research partnership with a U.S. university to study AI, among other topics. Over the next year, iFlyTek developed relationships with several other U.S. universities, all in the name of conducting fundamental research on machine learning and AI. In 2019, due to concerns about U.S.-origin items being used to commit human rights abuses, iFlyTek and seven other entities were listed on the Commerce Department's Entity List, a list of parties that an interagency group has determined pose a significant risk of being involved in activities contrary to U.S. national security or foreign policy. And earlier this month, iFlyTek was identified by BIS as one of 28 companies on the Entity List whose activities are of such national security concern that additional license requirements now apply. In short, any advanced AI chip produced anywhere around the world now requires a license if destined to iFlyTek because of the foreign direct product rule.

But even before iFlyTek was listed, it was risky to deal with. It presented a number of red flags, all of which could be found through open-source reporting or a Google search. We ask that if you find these red flags – like a connection to programs that enable human rights abuses or WMD development, close ties with state security services, or public reporting by Human Rights Watch or other NGOs – and there is a potential for technology transfer either through a deemed export or traditional export, you alert BIS either through the submission of a license application or by reaching out to one our OEE agents.

In addition to vetting your industry partners, we also ask that you review your academic institution partners for any red flags. Just this week, the Department of Justice indicted four Chinese nationals, including three alleged MSS intelligence officers, in a conspiracy to target professors at U.S. universities with access to sensitive information and equipment. The charges allege that the MSS officers did so using the cover of a purported academic institute — the Institute for International Studies — at Ocean University of China. Last year, we had a defendant plead guilty to illegally exporting sensitive U.S. technology – including anti-submarine warfare products – to Northwestern Polytechnical University, which has been on the Entity List since 2001. Northwestern Polytechnical is a Chinese university that is heavily involved in military research for the People's

Liberation Army and is considered one of the "Seven Sons of National Defense" public research universities that are closely tied to the Chinese military.

As another example, we recently added the Harbin Institute of Technology, or HIT, along with several of its subsidiaries, to the Entity List for using U.S. technology to support the PLA. At the time, HIT had a joint education program with a prominent U.S. university and academic exchange programs with several other U.S. universities. It also beat out MIT and Stanford to take a top spot for electrical and electronic engineering, according to the U.S. News & World Report's most recent "Best Global Universities" list. Despite this veneer of legitimacy, HIT was using U.S. technology to support Chinese missile programs.

Look, we understand that when it comes to complying with the export rules, universities rely heavily on their export management and compliance teams. That's as it should be. But we also want to ensure that the people on the ground – the professors, students, researchers, and staff – are paying close attention to these issues too and understand when to ask the specialists for help. Not all universities have an equal risk profile. Some universities have strong ties to the Department of Defense to develop emerging and strategic military technology. Some spend billions – yes, billions – of dollars per year on research and development. Others are still in the nascent stages of developing an export compliance program. Still others have no formal compliance program at all. My message to you today applies regardless of where your institution falls on the spectrum. We want to ensure that your critical research is not being used to power a foreign adversary's military or fuel their human rights abuses. And we want to work with you in that effort. Export controls are a shared responsibility.

* * *

This past summer, we established a comprehensive effort – our "Academic Outreach Initiative" – to help academic institutions maintain an open, collaborative research environment in a way that also protects them from national security risk. The initiative has four prongs:

- Strategically prioritized engagement;
- Assignment of "outreach agents" to prioritized institutions;
- Background briefings; and
- Trainings.

I'll go through each prong in turn and describe how we've worked – and will continue to work – to implement them going forward. Let's call this a mid-semester self-evaluation.

First, we've strategically prioritized our engagement with the academic research institutions whose work gives them an elevated risk profile. These are institutions that: (1) possess ties to foreign universities that are on the Entity List; (2) are involved in R&D for the Department of Defense; or (3) are conducting research in sensitive technologies subject to the Export Administration Regulations (EAR) - for example, laboratories conducting applied research on emerging or foundational technologies. Earlier this summer, our Office of Enforcement Analysis identified twenty universities whose work potentially gives them an elevated risk profile based on one or more of these three criteria. That list of twenty includes universities covered by our Portland Field Office, which has responsibility for the Pacific Northwest. In August, I reached out to each of the twenty institutions to see if they would be interested in partnering with us. Happily, all twenty said yes. In September, our Under Secretary, Alan Estevez, sent letters to each prioritized university noting the importance of maintaining a strong compliance program to guard against the risk of unauthorized exports, deemed exports to foreign national students and scholars, or 'support' to prohibited end uses or end users. The Under Secretary will be issuing letters to additional universities on a rolling basis this Fall. Please know that whether or not your university is one that has been prioritized so far, we are available and eager to help, and we're committed to partnering with you to navigate the landscape of export controls.

Second, we have assigned an individual outreach agent to each of the twenty prioritized universities. These "outreach agents" serve as a dedicated point of contact for the university to help answer questions, build long-term relationships, and help prevent unauthorized exports of technology or source code. To minimize risk, academic research institutions need to have a sophisticated understanding of the EAR and how these rules apply to professors, students, staff, and visitors. I highly encourage you to reach out to your dedicated outreach agent, if you have one, and if not, to your local Export Enforcement Office (including our Portland Resident Office for those of you here locally), for any questions you may have related to export enforcement. For questions about developing a strong export compliance program, you can reach out to our Office of Exporter Services and they'll be eager to assist.

Third, we will offer background briefings. We know that research universities often benefit from having strong working relationships with foreign universities or partners in industry. Sometimes, however, those foreign universities or companies can have ties to foreign governments, or other foreign actors – ties the U.S. university may be unaware of. Where appropriate, our outreach agents will brief universities on known national security risks associated with specific foreign entities or efforts by foreign adversaries to acquire specific technologies that are directly relevant to that particular university. We understand specific information related to potential export control risks or requirements can help inform your decisions.

Finally, we will offer trainings. Our outreach agents and analysts will offer trainings to prioritized academic research institutions on how export controls apply in academic settings and on ways to identify the national security threats facing academic research institutions. We will begin with a centralized briefing to our 20 partner universities on identifying red flags and mitigating risks, followed by a webinar on conducting open-source research. We will be offering the centralized briefing twice this fall, with the first one scheduled for tomorrow. In December, we will provide the additional training session on how to best conduct open-source research to better vet potential partners. That way, you can avoid ending up on the pages of our aptly named publication, "Don't Let This Happen to You" (which we just updated a few weeks ago with the most current case examples – the newly revised version is available on our BIS enforcement website). We are also coordinating with our Export Administration colleagues to provide a broader training for practitioners on regulatory requirements, which will be provided in the new year.

* * *

In short, we're committed to partnering with you to protect national security and to maintain U.S. leadership in innovation and collaboration. As the National Security Advisor recently said, we need to invest in the underlying sources and tools of American power and influence – especially our strength here at home – both for the purpose of effective competition and for the purpose of solving shared challenges. One of the most important sources of American strength at home is our innovation base, which has long underpinned both our economic prosperity and our military strength. The importance of collaboration, of a free and open exchange of ideas, is one of the bedrock principles of American society and has led

to our technological leadership. At the same time, though, we must ensure that our strategic competitors cannot exploit foundational American technologies, know-how, or data to undermine our security.

We are hopeful that our progress on the four components of our Academic Outreach Initiative will help empower universities to continue to drive innovation while also protecting national security. But we are only at the beginning of this effort. Your input will help us refine and improve our approach as we work together to both facilitate and protect U.S. technological leadership. In conclusion, we look forward to directly engaging with you – and your compliance teams – as we work to safeguard your critical research from improper foreign acquisition.

I'd be happy to take your questions.

For more information, visit www.bis.doc.gov.

###
