FOR IMMEDIATE RELEASE
June 28, 2022
www.bis.doc.gov

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

Assistant Secretary for Export Enforcement Matthew S. Axelrod at the National Association of College and University Attorneys 2022 Annual Conference
Pittsburgh, Pennsylvania
June 28, 2022
Remarks as Prepared for Delivery

Export Enforcement Academic Outreach Initiative Policy Memo Available online here.

Thank you, Ona, for that kind introduction. And thank you to the National Association of College and University Attorneys for hosting me today. It's terrific to be with all of you here in Pittsburgh.

In 1999, my wife, who had just graduated from business school, joined a small tech start-up in Cambridge, Massachusetts. When friends and family would ask what the company did, she would dumb it down for them, saying simply, "we make websites download faster." Today, that explanation might not resonate. But back in 1999, websites didn't load instantly. And the more photos or graphics they had, the longer they took. So, the ability to make websites download faster was something even my parents could understand. It was a service that was quickly adopted by some of the biggest websites in the country – sites like CNN and Yahoo. And today, twenty-plus years later, that small start-up, Akamai Technologies, is the largest content delivery network in the world.

Akamai's story is a profoundly American story. A start-up venture with innovative technology that meets a pressing customer need, which grows over time into a major industry player. But it's a profoundly American story in another way as well – none of it would have ever happened if it weren't for the collaborative environment of the American research university.

Akamai only exists because MIT exists. It only exists because one MIT professor, Tim Berners-Lee, the inventor of the World Wide Web, challenged other MIT professors to see if they could help address the problem of slow Internet download speed. It only exists because a MIT applied mathematics professor, Tom Leighton, then collaborated on that problem with his graduate students, one of whom, Danny Lewin, helped him come up with algorithms that routed web traffic more efficiently. And it only exists because Leighton and Lewin then collaborated with a MIT business school student, Jonathan Seelig, to create a business plan to commercialize the algorithms. They entered that plan in the business school's annual $50K entrepreneurship contest. They didn't win the contest, but they did well enough to attract venture capital funding

that turned the business plan into Akamai Technologies, a company that later went public with a market cap of over $13 billion.

I tell you that story not because it's singular. On the contrary, I tell it because it's emblematic of the contributions of both professors and students, in collaboration, to incubate innovative ideas and entrepreneurial solutions. Academic research institutions are a fundamental component of the scientific and technological success that forms the foundation of the American economy. Our colleges and universities are where life-saving medicines are developed, scientific breakthroughs are made, and revolutionary technologies are invented.

That innovation is driven by this country's open and collaborative academic environment. That open environment ensures that the best minds – from both the United States and abroad – can collaborate and share ideas. We want international students to study here because a diverse, international talent pool strengthens our economic and technological competitiveness. By some estimates, immigrants account for a quarter of the inventions and entrepreneurship that occur in the United States. What's more, it's estimated that, during the 2020-2021 academic year, international students studying at U.S. colleges and universities contributed $28.4 billion to the U.S. economy and supported more than 300,000 jobs.

At the same time, however, this open collaborative environment at our academic research institutions can create important vulnerabilities to our national security. American research universities aren't just the envy of the world, they're the envy of the parts of the world we consider adversaries. Our foreign adversaries know how successful our research universities are at developing the latest and greatest technologies, or medicines, or scientific innovations. They also know that, given the multitude of disciplines, heterogeneous makeup of professors and students, and open collaborative environment, a university's technology and research controls may not be as robust as those of a for-profit corporation – even though the research being conducted at universities can be just as valuable (if not more so) as that being done at companies. In a world where even the most sensitive and valuable research can be exported with the click of a button, our research universities unfortunately present inviting and potentially vulnerable targets. And it's that tension – between the genius of our collaborative university research environment and the national security challenges that environment can present – that I want to explore with you today.

This year marks the 40th anniversary of the Bureau of Industry and Security's Office of Export Enforcement, or OEE, which – thanks to President Biden, Secretary Raimondo, and the United States Senate – I now have the honor to oversee. For forty years, OEE Special Agents, aided by our intelligence analysts and export compliance specialists, have been on the frontlines of protecting U.S. national security, ensuring that sensitive U.S. goods and technologies aren't falling into the wrong hands. For much of those forty years, the focus was primarily on physical goods: commodities capable of civilian use but also capable of use in conventional weapons or in weapons of mass destruction, such as nuclear weapons, missiles, and chemical or biological agents.

As the pace of technological development has increased, however, the national security threat has evolved – and so too have our areas of focus. While traditional threats of conventional arms and the proliferation of weapons of mass destruction remain ever-present, new and emerging technologies have now joined them as primary areas of concern for us.

Each year, the Office of the Director of National Intelligence, or ODNI, publishes the Intelligence Community's Annual Threat Assessment, which details ODNI's view of the gravest national security threats faced by the United States. In its most recent 2022 report, ODNI identifies the "rapid development of destabilizing technologies" as one of the "transnational challenges [that] stand out for the clear and direct threats they will pose to U.S. interests during the coming years." As the report further explains, "The increasing convergence of seemingly unrelated fields and the rise of global competition to generate and lock in advantage are leading to a global diffusion of emerging technologies, shrinking timelines for development and maturation of technologies, and increasingly blurred lines between commercial and military endeavors, particularly in fields with broad impact across societies and economies, such as artificial intelligence (AI), biotechnologies, robotics and automation, and smart materials and manufacturing."

What this means is that technological development done at our research universities – work that can lead to the formation of companies like Akamai – can also increasingly lead to national security risks, especially because it can sometimes be difficult to determine the potential nefarious end uses of these nascent technologies until they are actually leveraged by malign foreign actors. If we can't effectively identify, control, and safeguard these emerging and potentially disruptive technologies, real national security risks result.

Let's start with just one of those technologies, artificial intelligence, to illustrate the challenge. AI technology has rapidly spread worldwide. It has improved how we integrate information, analyze data, and make decisions. Government, academia, and industry have all experienced its benefits. Like all tools, however, AI can also be put to harmful uses. AI-enabled surveillance tools have been developed that can monitor, track, and surveil people, thereby allowing authoritarian regimes to violate their citizens' human rights. There have been shocking headlines that describe how Chinese authorities have installed invasive mass-surveillance software in the Xinjiang province to track members of the Uyghur Muslim minority and map their relations with friends and families. Other stories recount how Russian authorities are ramping up the use of AI in facial recognition technology to track opposition protesters to their homes and arrest them.

While these examples may seem distant from the research occurring on your campuses, some of the AI companies behind these tools of repression, companies such as iFlytek and SenseTime, have past ties to U.S. research universities. Both companies are now 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 which means they can no longer easily access U.S. goods or technologies. But even before that legal hurdle was put into place, these companies were risky to deal with. Risky because of their connection to Chinese military, intelligence, and police organizations. But also risky to the reputations of universities who chose to engage with them.

And it's not just AI where universities face potential reputational and legal risk when working with foreign parties on the latest technologies. We had a recent case where a U.S. university received a grant from the National Science Foundation to establish a partnership with a foreign company, called CloudMinds, to develop a deep learning laboratory – that is, a laboratory that explores machine learning to analyze large data sets and develop prediction models. While CloudMinds may have seemed innocuous at first, its products were later identified in open-source materials as directly supporting China's military modernization efforts. What's more, the company's owner had an associated company that was described as the Chinese government's answer to DARPA, our defense agency that invests in technology development for national security purposes. Once we informed the university of the national security risk, the university took steps to end the collaboration. CloudMinds too is now on our Entity List.

Partnerships like this are just one of the ways foreign adversaries can attempt to gain access to cutting-edge research developments. Another involves attempts to exploit known relationships between U.S. universities and government research entities, such as Department of Defense-supported University Affiliated Research Centers, or UARCs. UARCs – strategic DoD research centers affiliated with a university – are often where the emerging technologies of tomorrow are being incubated. These nonprofit organizations are tasked with maintaining essential research and developing core capabilities in areas of particular importance to national defense. DoD has been cataloguing unsolicited requests to UARCs made by foreign researchers, and by foreign-entity-linked shell companies here in the United States, for information about emerging technologies being developed at UARC facilities. DoD has then been mapping those requests back to our adversaries' strategic military technology gaps to see where there is overlap between those gaps and the information requests. The preliminary results have been both illuminating and concerning given the volume of solicitations they're seeing and the tactics that are being used to obscure foreign military affiliations. For those of you whose institutions support UARCs, these dynamics raise particular challenges in implementing an effective compliance program over a broad swath of research activities and university personnel.

So now that I've attempted to describe the risks – both to your institutions and to our national security – what can we collectively do to help mitigate them?

The good news is that the vast majority of technology released in an academic setting is not subject to the Export Administration Regulations, or EAR, because it is released as part of classroom instruction or constitutes information that is tied to fundamental research. While certain inputs to, and results of, fundamental research may be subject to the EAR, most information that is tied to fundamental research – basic and applied research that is ordinarily published and shared broadly within the scientific community – is not.

What those of us at Export Enforcement are particularly concerned about is proprietary research. Proprietary research, which consists of research restricted from publication because it is considered confidential from a business or national security perspective, is generally controlled for either traditional export or "deemed export" purposes. While a traditional export involves sending technology from the United States to another country, a "deemed export"

involves the transfer of technology *within* the United States to a foreign national or non-permanent U.S. resident, through things like a briefing or hands-on laboratory research. Under the EAR, if a license would have been required to send that technology to another country, then a "deemed export" license is generally required to release such technology in the United States to a professor, student, or visitor whose most recent citizenship or permanent residency is in a foreign country.

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 develop an Export Management Compliance Program, or EMCP, if you haven't already done so. Our Office of Exporter Services is available to advise you on the creation and implementation of EMCPs that are tailored to your specific needs.

Having an effective EMCP will help you integrate export control requirements into everyday operations, which in turn helps minimize risks of violations. One key element of an EMCP involves a Technology Control Plan to safeguard sensitive information from unauthorized release. Another is conducting a risk assessment before engaging with foreign parties, starting with the screening of those parties against the U.S. Government's Consolidated Screening List – a list that, as the name suggests, combines all export-restricted parties identified by the Departments of Commerce, State, and Treasury in one place. In one past case of ours, a U.S. university was fined for exporting an atmospheric testing device to the Pakistan Space and Upper Atmosphere Research Commission, which was on the Entity List due to its involvement in Pakistan's nuclear and missile activities. Because of that Entity List status, the university was prohibited from shipping the device without a license, something the university could have easily determined had it conducted a screening check.

Another key element of an effective EMCP is having a system of information barriers and access controls in place to guard against the inadvertent release of controlled software or technology to specific faculty, staff, students, or visitors without the requisite license. Examples of such information barriers include physical locks and access procedures for entrance to research areas with controlled technology, as well as restrictions on access to controlled electronic files and software using personal identification verification cards and passwords.

So those are a few suggestions for what you can do on your end. But what about my end? What can those of us at the Department of Commerce do?

The challenges of keeping our academic research environments thriving and our controlled information secure from improper foreign acquisition are significant. That's why I'm announcing today a new Export Enforcement initiative to help academic research institutions protect themselves from these threats. This new "Academic Outreach Initiative," which is described in further detail in a policy memorandum that I sent earlier today to all Export Enforcement personnel, and which we are also making public, contains four lines of effort:

First, we will strategically prioritize engagement. While we are always available to any research university that wants our assistance, we will be specifically prioritizing for engagement those universities whose work has resulted in an elevated risk profile. These are institutions that: (1) are involved in research and development for the U.S. Department of Defense; (2) have ties to foreign universities that are on the Entity List; or (3) are conducting research in sensitive technologies subject to the EAR (for example, applied laboratories conducting proprietary research on emerging technologies).

Second, we will assign "Outreach Agents" for prioritized institutions. For prioritized universities that wish to partner with us, we will assign Export Enforcement agents to serve as "Outreach Agents," so that each prioritized university has a dedicated point of contact. Outreach Agents will seek to establish long-term partnerships with universities to help them prevent unauthorized exports, including improper releases of technology or source code. Outreach Agents will seek to meet regularly with their university counterparts, not less than once per quarter.

Third, we will offer background briefings. We know that research universities often benefit from having strong working relationships with foreign university or industry partners. Those relationships can be important sources of collaboration and innovation. Sometimes, however, those foreign partners can have ties to foreign governments, or other foreign actors, about which the university is unaware. Where appropriate, our Outreach Agents will seek to brief their partner universities on known national security risks associated with specific foreign entities.

And, fourth, we will offer trainings. For prioritized research institutions, we will offer trainings on how export controls apply in academic settings and on applicable national security threats. In addition, our Outreach Agents will offer hands-on training to help ensure those institutions know how to vet potential partners to determine connections to parties on the Entity List or that are otherwise of concern. Our colleagues in BIS's Office of Exporter Services will be available to advise on establishing and implementing tailored EMCPs. And we will provide a list of resources to help administrators, professors, staff, and students comply with the export rules.

In short, we at Export Enforcement are committed to partnering with you to protect national security and to maintain U.S. leadership in innovation and collaboration. We are hopeful that the four prongs of our Academic Outreach Initiative will empower colleges and universities to prevent unauthorized exports, including releases of controlled technology, and to make informed judgments about their future and ongoing partnerships with foreign universities and companies.

I said earlier that the story of Akamai is a profoundly American story. There's one additional aspect of Akamai's early years that – unfortunately – is part of our American story as well. Danny Lewin, the MIT graduate student I mentioned who helped discover the algorithm that became the "secret sauce" of Akamai's technology, co-founded the company in 1998. He died just three years later, on September 11, 2001. He was a passenger on American Airlines Flight 11 – the first of the four planes to be hijacked that day. Lewin, who had grown up in

Jerusalem and served in the Israel Defense Forces before coming to MIT for graduate school, used his military training to attempt to stop the hijackers from taking control of the airplane. He died trying as he became one of the first people the terrorists murdered that day.

The national security threats facing the United States are real and they are persistent. And while they have morphed significantly since that tragic day in 2001, they have not diminished. They continue to demand our collective attention and resilience, for colleges and universities perhaps in a way even greater than ever before. Twenty years after 9/11, the current ODNI threat assessment, which I referenced earlier, no longer lists terrorism as the preeminent national security threat. Instead, it assesses that the most significant threats now come from nation-state actors – China, Russia, Iran, and North Korea foremost among them. And because of the resources and strategic vision of these countries, they represent the most sophisticated threats to technology protection we have seen in OEE's forty years of existence – including the protection of technology developed at your research institutions.

Thank you to NACUA for inviting me here today and to all of you for your work in keeping your institutions vibrant and secure. It is my hope that BIS can serve as a resource to you going forward, to help protect the security of your institutions' research while continuing to support the incredible innovation and collaboration for which our universities are deservedly renowned.

I'd be happy to take your questions.