



**Bureau of Industry and Security**  
U.S. Department of Commerce  
*Where Industry and Security Intersect*

FOR IMMEDIATE RELEASE  
January 28, 2022  
[www.bis.doc.gov](http://www.bis.doc.gov)

BUREAU OF INDUSTRY AND SECURITY  
Office of Congressional and Public Affairs  
Press Contact: [OCPA@bis.doc.gov](mailto:OCPA@bis.doc.gov)

## **Opening Remarks by Assistant Secretary of Commerce for Export Administration Thea Kendler to the 2022 Massachusetts Export Expo**

*As prepared for delivery*

Good morning. It's a pleasure to be with you today, at least virtually. I want to thank Paula Murphy and the team at the Massachusetts Export Center for the invitation. They have been great to work with. This is my first presentation as Assistant Secretary of Commerce for Export Administration. In this role, I lead the Export Administration arm of the Bureau of Industry and Security (BIS).

I'll start by sharing some Massachusetts export data. In CY 2021, BIS approved almost two thousand license applications from Massachusetts, with a value of \$8.2 billion. We approved about 90% of the applications we received. That's the third most application approvals in the entire country behind California and Florida.

Given that, I gather most of you are familiar with BIS's work, but I don't expect you're all that familiar with me. I'd like to start today by taking a few minutes to give you a bit of a sense of who I am, my approach to this role, and some of my priorities at the outset. I will get to the regulatory updates you're all waiting for, and I look forward to taking some questions as well.

To start with, I am a national security lawyer. I have over 20 years' experience in export controls, first at a private law firm, then in the BIS counsel's office, and most recently at the Department of Justice as a criminal prosecutor.

For the last seven years, I was in the Counterintelligence and Export Control Section of the Justice Department's National Security Division. I've worked on dismantling procurement networks, thwarting intelligence threats, deterring economic espionage, and holding criminals accountable for breaking the export control laws that you work so hard to comply with.

As a criminal prosecutor, I saw firsthand that our export controls work. Bad actors that can't have lawful access to U.S. technology try to obtain it illicitly.

One case I worked on involved a Chinese intelligence officer who tried to covertly obtain jet aircraft engine technology. You know we require a license for this tech to China. He targeted leading U.S. and international aviation companies. And recruited the companies' aviation technology experts to come to China for "exchanges" during university lectures and conversations with academics. But the audiences in China were Chinese government officials who sought the technology. Even though this scheme fortunately did not result in the unlawful export of controlled technology, I raise it because it further opened my eyes to the concerns facing you and your companies. You are thinking seriously about theft of trade secrets, which may very well be export controlled.

I also was part of the team that charged the telecommunications company Huawei with operating as a criminal enterprise, stealing trade secrets, and defrauding global financial institutions. The Huawei Indictment notes that had Huawei's banks known about the company's repeated violations of the Iran sanctions, they would have reevaluated their relationships with Huawei. According to the allegations, the banks continued banking Huawei and its affiliates based in part on Huawei's false statements. This is another example of our export controls and sanctions laws fulfilling their intended purpose. Financial institutions and other companies are focused on compliance and can be duped by bad actors trying to evade controls.

One final story – another case that was meaningful to me: As you probably know, we have significant controls on radiation-hardened integrated circuits – including those in ECCN 9A515.e.1 for those who like the details – going to Russia. According to an indictment I worked on, a Russian individual tried to obtain these chips from a U.S. company and was told that export controls barred the shipment. So instead, as we alleged – with co-conspirators – he set up a company in Bulgaria to receive the chips and send them on to Russia. He is also alleged to have used the front company to obtain almost \$2 million in U.S. electronic components for shipment through Bulgaria, where they were repackaged, and on to Russia. Bulgaria, of course, is a NATO member and under Country Group A it receives favorable export controls treatment.

I'm sorry to say that the U.S. rad-hardened chip manufacturer was witting in this scheme. They agreed to pay just short of 500 thousand dollars as a civil penalty and they're now the subject of a suspended denial order. Unfortunately, they knew about the need for the chips in Russia and the planned "business model" in Bulgaria.

Our export controls work. We're implementing national security, foreign policy, and economic security goals through the EAR, and we see that bad actors can only resort to illicit procurement. Fortunately, my colleagues in Export Enforcement and across the U.S. law enforcement community are very good at what they do.

These cases, and much of my other work at the Justice Department, gave me direct experience with the challenges American businesses – large and small – face when it comes to determined efforts to evade export controls. I bring with me to my new role as Assistant Secretary a clear view of the environment in which we operate.

I want you to know that I approach export control matters seriously and judiciously. We will follow the facts when it comes to identifying national security threats and applying export controls. We will ensure our rules are effective and reflect our changing world.

As much as my national security experience will inform my approach to this job, so will my values. I have always felt a deep gratitude to the country that provided my family with the opportunity to prosper. My commitment to public service generally, and national security specifically, flow from that gratitude.

My mother and my grandparents came to our country after World War II as refugees. Through determination and hard work they achieved the American dream within one generation. My mother went on to a long and successful legal career of public service as an attorney for the State of New Jersey. My father, a university professor, which I also think of as a form of public service -- inspired me to understand the world and see current events from multiple perspectives. I was raised in an academic community that valued international collaboration and a true exchange of ideas. We lived in Japan when I was a teenager, and I studied foreign languages, including in Beijing. I'm fortunate to have been supported by a family that exposed me to so much. I feel a keen responsibility to give back and to contribute to the security and prosperity of the people and country that gave us so much.

Preserving that security and prosperity means standing up for the principles of adherence to the rule of law, advancement of human rights, multilateral engagement, and democratic governance. I'm proud to be part of an Administration that has placed these principles at the heart of its agenda. Right now, we face new challenges to our security and prosperity. We are seeing national security, foreign policy, and economics intertwine like never before. Authoritarian regimes and non-state bad actors seek to turn the strength that is our economic prosperity, into a weakness they can exploit. Many of you know this reality too.

I come into this job clear eyed about the threats we face—but I am also confident in the extraordinary people I'm humbled to lead, and the mission we're charged to carry out. I believe deeply in BIS's mission to advance America's national security, foreign policy, economic competitiveness, and technological leadership through effective export control policies. This mission—and the unique role BIS plays in the constellation of federal agencies to fill it—could not be more relevant.

Major diplomatic discussions between countries and debates about military strategy are usually somewhat abstract. They happen at summits in Geneva, or in the White House Situation Rooms. They are important—maybe intimidating and high stakes—but not reality for most of us. BIS connects these strategies and debates with the activities of the American people and American businesses. We bring a unique perspective to these conversations within the government and with other governments—our experience with people who are in the marketplace every day.

You.

Our work with you and exporters across the United States gives us a deep understanding of the economy. The work it takes to bring products to market. The R&D that goes into new technology. The impact that decisions in Washington, or Brussels, or Beijing have on how you operate and what that means for your workers, their families, and communities. BIS applies a national security lens where it matters to the underlying strength and health of our nation— informed by the commercial relationships you’ve built, the innovation environment you’re advancing.

At BIS we think about the products and the engineering, the global threat picture, the market, R&D funding, foreign availability, and more. We don’t just think about “what if”—we have to consider “what is.” And we avoid restrictions that hurt the international competitiveness of U.S. industry unless there are real national security benefits. We base our decisions on data and facts. We have worked at the nexus of national security, foreign policy, economics and technology for decades.

Authoritarian regimes and non-state bad actors are seeking to turn commerce into chaos. It’s a playbook that I saw clearly as a prosecutor, and it’s the threat environment for BIS and our intra- and inter-government partners. Our non-proliferation concerns have not changed: missiles, chemical and biological weapons, nuclear capabilities—these are still serious concerns. And we have strong institutions, alliances, and partnerships that agree on those points -- that help detect and deter malign uses of those technologies. We live in a changing world, and our traditional, regime-based, approach cannot help us adjust to every scenario.

We are increasingly using the Entity List to identify entities of concern for you – so that you know which specific transactions need extra scrutiny. We’re similarly identifying Military End Users in certain countries for which additional license requirements apply for certain items.

We also are prepared to act quickly, and unilaterally when conditions warrant. For example, in 2020, we issued a unilateral control for certain software specifically designed to automate the analysis of geospatial imagery under our 0Y521 ECCNs. While artificial intelligence (AI) is an important technology that is frequently being used in more commercial products and services, this specific application of AI with geospatial imagery presented national security concerns. We found that the U.S. was the sole developer of this type of software. As a result, we proceeded with the 0Y521 control. We are pursuing a multilateral approach to controlling this technology through Wassenaar, but it is an example where we needed to lead and act quickly to address national security and foreign policy concerns.

I understand that research and innovation are essential and international collaboration may be necessary. I also understand how essential it is for U.S. companies to actively participate in international standards organizations. Our commercial ties with like-minded partners support a vibrant economy here at home and enhance our global security posture.

Technology is tightening the connection between national security, foreign policy, and economics. We have to stay ahead of the threats. National security is a shared responsibility—we all need to do our part. That is key to my approach to this job. That we work with our federal partners. We work with our international partners.

Importantly, we will work with you. Because day-to-day, whether you think of it this way or not, you are the front lines of our national security. You see the market demands and screen your shipments. You know your customers. You're creating the new products and technologies that create new jobs and opportunities, drive our economy, and enhance our security. You're engaging with foreign and domestic partners in the private sector every day. That daily engagement, your practical insights and partnership is essential to BIS.

I am always hungry for data, and for practical solutions to our shared responsibilities. As much as you seek guidance from us, I'm going to be seeking guidance from you. We are in this together. I want you to know that my door is open, and I look forward to hearing from you.

Let me turn to a few priority areas that I look forward to working with you all on.

First, we must use our export controls to ensure that your technological innovation is not diverted to destructive ends that hurt our national security.

This means using export controls effectively to confront and combat China's military-civilian fusion program. Deterring Russia from taking aggressive and dangerous actions. Continuing to work with our multi-lateral partners to restrict nuclear, chemical, and biological technologies to prevent them from being diverted to weapons of mass destruction and terrorism. The list of threats and malign actors is long, and the threat environment is ever changing. But we are leading with our values and working together with like-minded partners in the government, the private sector, and outside the United States.

Second, we must tailor export controls to ensure that we don't disincentivize your technological leadership and that we return resources to the United States for further innovation and research. Our universities are the envy of the world because we welcome the brightest minds from anywhere. Our companies innovate and create jobs because they engage across the globe. Our public policies and laws are transparent and the product of open—sometimes raucous—debate. The openness of our economy and society must remain a strength. And you must be able to sell your technology to foreign markets so that you can continue to innovate. BIS will work to use export controls effectively, judiciously, and whenever we can in concert with like-minded allies. This approach is particularly important in the areas of emerging and foundational technologies.

Finally, we must make our export controls a multilateral – or plurilateral or bilateral – system as much as possible. Unilateral controls have a place in our system, but we know that they affect you and not your foreign competitors. We must use them judiciously. I will use my platform to continue pushing for partner countries to recognize our national security concerns and join us in similarly applying controls.

As I mentioned, I like data. BIS does the hard analysis, we collect the information, and we consider both “what if” as well as “what is.” We have to look at the whole picture. I'm so proud of BIS's analytical capacity. It enhances our export controls work, helps us understand our industrial and innovation base, and enables cooperation to promote a competitive environment for innovation and experimentation.

Semiconductors are ubiquitous, and essential to nearly every facet of modern life. Our bodies need food and water—nearly everything else needs computer chips.

BIS understands that. We contributed substantially to the Department of Commerce’s analysis of semiconductor supply chain risks as part of the Administration’s report under Executive Order 14017. That report included analysis of the global semiconductor industry. It assessed supply chain risks. It also outlined recommendations for industry and government to work together to secure our long-term leadership in the sector—something that I will be intensely focused on. That’s just one example of the type of detailed, clear-eyed analysis, coupled with action, that BIS can take to support and grow our industrial base and support innovation.

We identify national security threats. We need you—our front lines – to help us understand the current economic environment—domestically and globally—and ensure our export control rules and policies are informed by the reality of the marketplace. We will continue to be as transparent as we can with you, sharing as much as we can about the threats that we address. And I hope you will take me up on my request for information so that I can see the whole picture.

I am fortunate to be taking this role at a moment when BIS has been working hard on all of these fronts. It’s an exciting time to be back at BIS – I’m very glad to be here.

###

[Regulatory Update Export Expo](#)