Under Secretary of Commerce for Industry and Security
Alan F. Estevez
Keynote Remarks
BIS Update Conference 2024

As prepared for delivery

Good morning and welcome to the 2024 BIS Update Conference on Export Controls and Policy. I'm thrilled to be here once again to kick off this three-day event with you all.

Before diving into things, I want to thank Karen Nies-Vogel and the Office of Exporter Services for pulling everything together for this event. This is our first time hosting entirely in person since the COVID-19 pandemic, and although it's certainly refreshing to feel like we're somewhat back to normalcy, I know it required a lot more from Karen and the team—so thank you.

Our last Update Conference was in June of 2022. A lot has happened in the export control space since then.

I want to briefly thank all of the members of the BIS team for their hard work—the volume and tempo of our work have been incredibly high, and we're able to sustain those efforts only because of the dedicated professionals of the Bureau.

Today, I will touch on the current export controls context, review some of the major work we've undertaken since the last Update Conference in 2022 and share some insights on where things are headed.

Export Controls Evolution

As those of you in this room know, BIS has operated for decades at the nexus of national security, technology, and commerce.

The growth in the importance of export controls as a national security tool mirrors the dynamic of militarily useful technology. This transition has been going on since before the Berlin Wall came down. Through the 1980s, military dollars largely drove research and development in the United States. Even when you look specifically at the semiconductor space, originally, the Department of Defense was the main buyer of semiconductors. Of course, that has reversed; the defense industry ecosystem now looks to the commercial sector for innovations that are useful. Technology and commercial research and development from the private sector are the driving forces behind the innovation ecosystem.

Especially given the rapid state of technological progress, export controls cannot be static. There is no magic single control that we can put in place that will forever stop our adversaries. Export controls are about impeding access, increasing costs, and countering efforts to evade our controls. We have to continually evaluate the global security context and the technological landscape, and we need to update controls accordingly.

As is often the case, things happen gradually—then seemingly all at once.

That is the story of the past few years.

Over the past two plus years, we have taken significant actions to respond to Russia's full-scale invasion of Ukraine and to counter the threat from the People's Republic of China's (PRC) military modernization efforts.

We have worked closely with international and interagency partners to strengthen our multilateral ties both to counter these threats and to help shape more secure supply chains. The United States is the world's most powerful economy, but we aren't the only ones engaged in global trade—so our controls are most effective when we work together with other countries.

We have also worked incredibly hard to enhance our enforcement efforts. As Assistant Secretary Axelrod has repeatedly pointed out, our colleagues at Homeland Security Investigations have more agents in Tampa, Florida than he has in the entire world, and I am proud of our enforcement team's steadfast efforts to meet quickly growing demands.

From policy changes to greater collaboration with interagency and international colleagues, we are doing everything we can to leverage our resources with those of others in order to maximize our impact. Much of that work has occurred in just the last two years.

Russia/Ukraine

BIS has taken aggressive actions, in concert with 38 other allies and partners, to impose extensive export controls in response to Russia's full-scale invasion of Ukraine. This multilateral approach was critical, as the U.S.-Russia volume of trade was relatively small at the start of the invasion.

We continue to act aggressively to prevent Russia's access to the technology needed for its weapons. From February 24, 2022, to December 31, 2023, the Office of Export Enforcement (OEE) detained 559 shipments that were destined to Russia, valued at over $284 million. We also stood up a Disruptive Technology Strike Force to prioritize investigations involving diversions to Russia, China, and Iran. Many of these Strike Force cases involve Russian schemes to purchase critical dual-use technology, including military-grade components that could be used in missiles and UAVs.

BIS has also used the Entity List vigorously to restrict not only Russian and Belarusian entities' ability to obtain items to support their war effort but also entities in a variety of third countries. Since March 2022, more than 900 entries have been added to the Entity List, with 636 in Russia, 29 in Belarus, and nearly 250 in more than 30 third countries.

Many of these entities have also been added with a footnote 3 designation, which, through one of the Foreign Direct Product Rules, effectively cuts them off from being able to obtain additional foreign-produced items with U.S.-origin components or made using U.S. technology subject to the Export Administration Regulations.

Our actions have imposed increased costs on Russia. They have forced Russia to rely on pariah states, such as Iran and North Korea, for weapons. And they have forced Russia to expend resources to create networks to evade our controls. In response, we have implemented new controls targeting Iran and entities throughout the world who are violating our restrictions. We have also acted strongly with allies and partners to detect and disrupt those networks. We will continue working with our international partners to align on and enforce our controls.

We are also working with industry to enhance due diligence to detect efforts to evade our controls. No one wants American-designed items turning up in Iranian drones or weapons used by Russia to kill civilians in Ukraine or attack Ukraine's critical infrastructure. But it's happening. This is a global challenge, and we all need to do more and think creatively.

So, right now, we are partnering with the Departments of State and the Treasury to engage with the private sector to further restrict Russia's access to U.S. semiconductors. We are actively working with companies and other relevant stakeholders to ensure information about bad actors in the broader semiconductor distribution chains is disseminated so that these pathways to Russia can be shut down.

We are asking the private sector to step up more than it has, and even if you have not heard from us directly, we need you to be part of the solution. Traditional due diligence is not sufficient—especially if your company or your clients have complicated distribution networks. Government and industry both need to show a commitment at the highest levels and continue to devote resources to detecting red flags, vetting intermediaries, tracking controlled product, and sharing information and best practices.

While all of our efforts related to export controls are important, I want to be clear: The most important step the United States can take right now to help Ukraine is to provide funding to support the fight against Russia's invasion. New funding, along with other tools in our toolkit, will continue to impose costs on Russia and those who seek to support Putin's unjustifiable actions.

As I noted in my Congressional testimony last week—China is watching our actions and our willingness to stand up against illegal aggression. Helping Ukraine is also about China.

PRC

As the Administration's National Security Strategy and the Intelligence Community's Annual Threat Assessment make clear, the PRC represents the most significant challenge to U.S. values and security interests.

However, our relationships with Russia and the PRC are very different—so are the relationships between the PRC and many of our close allies and partners. There is a substantial amount of trade between the United States and the PRC that does not present national security concerns, and it is in our interest to continue to engage where we can.

I want to be clear: Export controls are a national security tool, not an economic protectionist tool. BIS has been called upon to apply export controls on items that the PRC is seeking to obtain in order to advance its military modernization and its human rights abuses.

We have long maintained controls on the PRC for military, spacecraft, and multilaterally-controlled dual-use items, as well as certain predominantly commercial items if used by military end users or in military end uses. As critical and emerging technologies have continued to advance, we have strived to keep pace. Military advantage is now being sought through advanced computing power—supercomputers that can manage and manipulate vast amounts of data, artificial intelligence (AI) that speeds military decision-making, and a host of other activities that rely on certain advanced chips and the ability to make or obtain them.

So, in October of 2022, we began implementing sweeping, strategic, country-wide controls on key types of critical and emerging technologies. These technologies include advanced computing chips needed to power military AI and supercomputing applications, as well as semiconductor manufacturing equipment essential to producing advanced chips. We then refined and expanded these controls in October of 2023. We will continue working to assess their impact and effectiveness, and we intend to revisit them regularly to protect U.S. national security and foreign policy interests, as appropriate.

This country-wide approach is important because we are identifying strategic sectors and items and setting clear lines based on technological capabilities. This is a more durable and effective approach than focusing solely on particular entities and case-by-case license reviews. We have already seen reports of constraints to the PRC's high-performance computing capacity and other areas that suggest our controls are having an impact.

However, in the case of our rules from October 2022 and 2023, we also understand that acting unilaterally minimizes effectiveness and creates an unlevel playing field for U.S. companies and can thus undermine U.S. technology leadership. History has shown that the United States often needs to lead, but this Administration places the highest priority on working with our allies to make sure we are not alone. This remains an important priority as we continue to assess these technology-based restrictions.

In addition to our countrywide controls, we continue to add PRC parties to our Entity List. In fact, we have added more than 300 entities during this Administration. These actions help to backstop our technology-based controls by denying PRC entities access to predominantly commercial items that could be used for military applications or human rights abuses. Over 100 of these entities have also been added for supporting Russia's military industrial base since the start of its war against Ukraine, and we will continue to use the Entity List to send a clear message to entities in the PRC and elsewhere that we will not tolerate engaging in activities contrary to U.S. national security and foreign policy interests.

We are also working hard to ensure that there are teeth to our controls through enforcement efforts.

BIS remains laser-focused on preventing sensitive U.S. technologies and goods from being used for malign purposes. In 2023, we issued our largest standalone civil penalty in history—$300,000,000—for Seagate's alleged violations of U.S. export controls related to selling hard disk drives to Huawei even after Seagate's only two competitors had stopped sales because of the Foreign Direct Product Rule.

We have also expanded our reach through partnerships. That is why we established the Disruptive Technology Strike Force in partnership with the Department of Justice last year. The Strike Force brings together experienced agents and prosecutors in seventeen locations across the country, supported by an interagency intelligence effort in Washington, DC, to aggressively pursue enforcement actions against illegal procurement networks and prevent nation-state actors from illicitly acquiring our most sensitive technology.

Recently, BIS agents and the FBI worked together on a case involving the theft of trade secrets, resulting in an indictment. The case involves a Chinese national who was employed by a large Silicon Valley company. During his employment, the defendant is alleged to have siphoned proprietary information related to AI while covertly working with two China-based companies seeking an edge in the AI technology race.

And in January 2024, four Chinese nationals were charged with various federal crimes related to a years-long conspiracy to unlawfully export and smuggle U.S.-origin electronic components from the United States to Iran that would ultimately benefit entities affiliated with Iran's Islamic Revolutionary Guard Corps and the Ministry of Defense and Armed Forces Logistics, which supervises Iran's production and development of weapons, missiles, and Unmanned Aerial Vehicles.

Evolving National Security Approach

The challenges to peace and stability that Russia and China pose have forced a revitalization of export controls—as well as an evolution to our approach and the addition of new, non-export control tools to BIS's toolbox.

How has BIS's approach evolved?

First, we are looking at export controls from a strategic perspective. We ask ourselves a number of questions. What are the specific national security or foreign policy concerns we are trying to address? Will the proposed control achieve our objectives? What will the impact be on U.S. technological leadership? Will the control create additional collateral consequences? Will allies and partners act with us? And is the control enforceable? These and other questions inform our strategic approach, and they have helped us carefully scope many of our actions, including the AI chip and semiconductor manufacturing equipment controls.

Second, over the past few years, we have engaged vigorously with our international allies and partners, and as I already mentioned, this is a key part of our strategic analysis. We owe our allies and the exporting public clear articulations of our national security or foreign policy concerns when we act. In the case of our Russia controls, this was easy due to Putin's unjustifiable invasion of Ukraine. In the case of new technology controls, this can be more difficult, especially when some of the technologies of concern are predominantly used for commercial applications. Having a shared threat perception is key to multilateral controls, as is effective enforcement of such controls by our partners, and we are continuing to prioritize these efforts.

While traditional multilateral export control regimes play a key role in ensuring international support for our actions, we must recognize that today's geopolitical realities, today's threats, and today's pace of rapid technological change require creative thinking and greater flexibility to protect the national security of the United States and our allies. In this regard, it has been encouraging to see allies examine the legal authorities they need to implement new controls outside of the multilateral regimes and to adopt new controls proposed at the Wassenaar Arrangement that were blocked by Russia. We will continue working to bring others on board and further align our controls as we seek to address additional critical and emerging technologies.

Third, even while we take a strategic approach to applying controls, we are not ignoring the need to address individual actors and to be aggressive in our enforcement posture. There are now more than 800 PRC entities on the Entity List, including more than 300 in this Administration. There are more than 900 entities on the Entity List related to Russia's invasion of Ukraine, including about 250 in countries outside of Russia and Belarus.

Fourth, we employ our other authorities—both old and new—alongside export controls to advance national security from other angles. We are using our survey authority under the Defense Production Act to provide critical insight into the use and sourcing of PRC-manufactured legacy chips in the supply chains of critical U.S. industries. To implement the President's AI Executive Order, BIS is proposing first-of-its-kind reporting requirements on companies that training of large AI models that could pose a threat to national security.

Nowhere is BIS's expanding set of national security equities more self-evident than in the Office of the new Information and Communications Technology and Services (ICTS) program. In 2022, BIS welcomed ICTS as a formal part of the BIS mission. The office of ICTS—or "OICTS"—is charged with protecting our nation's information communications technology systems from foreign adversary threats. Authorized under the International Emergency Economic Powers Act (IEEPA), the program has the authority to review, regulate, and restrict ICTS transactions that involve entities associated with foreign adversaries.

We have been busy growing the program, hiring the program's first Executive Director Liz Cannon, and initiating the program's first set of regulatory actions. Last month, in response to the growing involvement of the PRC in the supply chain for connected vehicles, BIS issued an Advanced Notice of Proposed Rulemaking related to security risks from foreign adversary technology in connected vehicles. As national security threats evolve, so does BIS. Going forward, ICTS promises to be an important part of the BIS mission.

Finally, BIS is not acting alone to advance U.S. national security. The Department of Commerce employs an "offense/defense" approach—BIS's work is the defense. The offense is the Department's work, led by other bureaus, to implement the CHIPS and Science Act and a host of other laws, which will ensure that U.S. technological leadership continues to advance and that the benefits of this advancement are widely distributed across our nation. This is part of the Biden-Harris Administration's whole-of-government approach to strategic competition with the PRC. By taking this approach to strengthening and enhancing our capabilities here at home and also working to coordinate with allies and partners, we are making it more likely that export controls will have an even greater strategic impact in the future.

Sustaining BIS's Efforts for the Future

These actions are just the beginning of BIS's ongoing efforts to protect national security, particularly as technology advances and we become an even more digital and connected society.

And as the technology landscape continues to evolve, BIS has been asked to do more in an era of strategic competition to address our national security and foreign policy concerns. We are proud of our recent accomplishments and the work we're doing to advance U.S. national security, but there's an opportunity to do so much more and to accelerate our impact. To meet this moment, there are a few realities that need to be confronted. Consider the following:

- When adjusted for inflation, BIS's budget for core export control functions has remained essentially flat since 2010.
- Yet during the same period, total U.S. exports have increased approximately 62 percent, and exports subject to BIS license requirements have increased approximately 126 percent since 2014.
- Our licensing workload has doubled from approximately 20,000 per year in 2012 to over 40,000 per year.
- BIS's law enforcement component employs only 150 agents to monitor the more than 30 million export transactions annually and counter the threat posed by nation state actors around the world.
- And our staff relies on antiquated systems, for both license adjudication and enforcement work, that were put in service in 2006 and 2008, respectively.

BIS and the Department are working with Congress—including many of the Hill staff in this room—to put BIS on the right path for boosting our central work in this new era of strategic competition.

Given today's threat environment, combined with rapid technological change, BIS's vital tools are increasingly being leveraged to protect the national security and foreign policy interests of the United States and our allies and partners.

We will continue to address the rapidly evolving pace of technological development and the threats posed by malign actors. Russia, China, North Korea, and Iran—as well as others—are desperately trying to obtain or produce advanced technologies for activities that present national security and foreign policy concerns.

BIS will continue working to be strategic in our actions and coordinated in our controls. We will relentlessly counter the threats of today and will adapt to address the challenges of tomorrow. And to that end, we look forward to working in partnership with you. Thank you for joining us.

###