Assistant Secretary of Commerce for Export Administration Thea D. Rozman Kendler Delivers Remarks at the WorldECR Forum

London, United Kingdom
December 3, 2024

Remarks as Prepared for Delivery

Introduction

Thank you to WorldECR and editor Tom Blass for including me in this terrific event, focused on trade control law and regulations, policy, and practice. I'm particularly glad to participate in the London version of this conference – my time as Assistant Secretary of Commerce for Export Administration in the Biden-Harris Administration has been marked by extensive cooperation and collaboration with my United Kingdom counterparts, so it's especially fitting that I'm here this week for my last international outreach during my tenure.

For three years now, I have led the part of the U.S. Commerce Department's Bureau of Industry and Security (BIS) that designs policy to control the proliferation of "dual-use" items. We are in a time of increasingly rapid evolution of both technologies and national security threats. This requires our team to even more nimbly identify technologies for which guardrails are necessary and amend our controls as appropriate.

Even as we conduct the traditional work of screening transactions and adjudicating license applications, our ever-changing environment places new demands on our ability to assess technical performance; review available intelligence on destinations, end users, and risk of diversion; and scrutinize end uses.

I am proud of what our team has accomplished during my tenure, and the creativity they have brought to their work in a resource constrained environment to protect U.S. national security and safeguard global peace and stability.

Biden-Harris Administration Export Controls Achievements

When I took on this role almost exactly three years ago, we established three clear priorities that have not wavered:

1. Degrade Russia's military capabilities and thwart Russia's unjustifiable invasion of Ukraine;
2. Impede the People's Republic of China's (PRC's) ability to modernize its military, a threat that is exacerbated by the Chinese Communist Party's Military-Civil Fusion (MCF) strategy; and
3. Deepen our export control relationships and coordination with our allies and partners.

Degrading Russia's Military

Russia has been at the forefront of the Biden-Harris Administration's policy decisions, and that is reflected in how I spent my first weeks on the job – and at least part of each week since then. Using our authorities, since February 2022, we increasingly ramped up our controls on Russia, its enablers in Belarus and Iran, and the DPRK. We published nearly fifty rules imposing a range of restrictions on Russia, controlling not just all items on our Commerce Control List but also around 2,500 lower-level (EAR99) technologies based on Harmonized Tariff Schedule (HTS) code. And we added over one thousand organizations in Russia and those who supply

Russia to our Entity List. This is what was expected of us in export controls, classic controls on items and entities.

It's an axiom in our field that export controls are only effective when other manufacturers of the same technology implement comparable controls – it's the premise underlying our four multilateral regimes and the plurilateral arrangements we've built in this Administration. In contrast, controls applied to items widely available from foreign sources generally are less effective. We know there are situations in which unilateral controls are necessary, especially when our values are at stake. But unilateral controls not only do not accomplish our national security goals, they also create an unlevel business environment for companies operating in – or in our case, for companies that produce technology in – the country that imposes the controls.

We confirmed the truth of this axiom as we crafted – and iterated – our response to Russia's invasion of Ukraine. We established closer than ever export control relationships with the UK, Japan, and the European Union. And we built on those relationships to form with 38 partners the Global Export Control Coalition that continues to coordinate controls targeting Russia.

It is *because* we reinvigorated our international partnerships that we created the possibility of even more effective controls. I'm continually impressed by how far the word has spread about our "Common High Priority List" (CHPL) for Russia, which comprises fifty Harmonized Tariff Schedule (HTS) codes at the six-digit level – the international language of trade. The CHPL was developed through careful analysis of the items Russia depends on for its military, including components recovered from the battlefield. If the United States had acted alone to create and disseminate this list, we might have convinced a number of partners to join us in extra controls on these items. It is *because* we worked with our partners that the list has worldwide recognition – not just by Customs services, but to the point that it has been adopted into the law of several partners.

Notably, HTS codes are Export Control Classification Number (ECCN) agnostic. Items like microelectronics, which top the CHPL, are controlled for Russia whether they fall under our advanced computing controls or are EAR99, commercial-grade legacy chips. This is a new approach to export controls, enabled only by our global approach. And we're grateful to our partners who share our concerns – consider, for example, Armenia, which adopted a law specifically requiring export licenses for these items going to Russia last year. Customs data shows that the average of CHPL exports from Armenia to Russia has fallen around 70 percent compared to the same period last year, and the latest data reported shows the lowest monthly total in exports to Russia since May 2021.

Thanks to this partnership, our coalition restricts thousands of items to Russia, and has cut off trade with much of the procurement network that feeds Russia's defense industrial base.

While we have pursued these government-to-government measures, we have also increased outreach efforts with U.S. industry to map out supply chains, assisting our efforts to completely cut Russia off from U.S.-origin and U.S.-branded components. The effectiveness of export controls, of course, hinges on the compliance efforts of industry. As you and our industry partners know, Russia continues to build sophisticated procurement networks to illicitly access U.S.-origin and branded components. And so, we continue to work with the private sector to ensure they know who the end users of their items – especially microelectronics – are, which helps industry strengthen its compliance and due diligence activities.

In this area, too, our team identified a creative way forward – we began adding addresses to our Entity List. This allowed us to specifically target corporate secretaries and shell companies, putting all parts of Russia's

global procurement networks on notice. Our partnership with industry, combined with information sharing with our government partners, results in increased visibility into Russia's procurement network that influences our rulemaking.

We have seen the impact of our actions on Russia, evidenced by Russia's frustration over its military ambitions due to increasing costs, delays, and reduction in equipment quality. And prices are driven up by the cost of establishing and re-establishing illicit procurement networks as we continue to disrupt them. Customs data shows that:

- Russia was forced to pay over **135%** more on average for microelectronics after the invasion than it did in the preceding years, based on average cost by weight.[1]
- Russia was forced to pay prices inflated by more than **320%** to procure advanced coalition origin machine tools via the PRC and Türkiye.[2]
- Russia was forced to pay over **210%** more to smuggle critical U.S.-origin items through third countries.[3]
- Our team – in close cooperation with our BIS law enforcement colleagues and partners throughout the U.S. and partner governments – constantly analyzes potential new avenues for Russia to evade our controls so that we can act swiftly to cut them off. Our partnerships with industry and coordination with partners and allies have, and will continue to be, essential in achieving that end.

We haven't just learned valuable lessons from our response to Russia, we've built new institutional muscle.

Impeding PRC Military Modernization

Principal Deputy Assistant Secretary for Strategic Trade and Economic Security Matt Borman has said that we spend "100% of our time on Russia, 100% on China, and 100% on everything else." It's true – we have a tremendous team, working at a backbreaking pace. This is doubly clear when we look at this Administration's actions in impeding PRC military modernization.

BIS has worked tirelessly to comprehensively restrict the PRC's access to tools and technologies for leading edge indigenous semiconductor production capabilities. This includes our "October rules" in 2022 and 2023, the April 2024 clarification rule, and the controls we announced yesterday on semiconductor manufacturing equipment.

I want to start by taking a step back to answer why all of these controls are necessary.

First, remember that we are operating in an environment in which the PRC's military-civil fusion (MCF) strategy is a whole-of-government, at-all-costs approach. Its goal is to ensure that innovations in the "civilian" sector advance PRC military capabilities. Together there, the strategy involves eliminating barriers between the PRC's (1) civilian research and commercial sectors, and (2) military and defense industrial sectors. To meet its objectives, the PRC has mandated and incentivized relevant domestic firms to dedicate significant resources sourcing foreign technologies that are relevant to military modernization with the goal of indigenizing their production in the PRC.

[1] Average value per kilogram of items under Tier 1 as reported in customs data, 3/2022 – 12/2023 vs. 1/2021 – 2/2022.
[2] Average value per kilogram of items under Tier 4.B as reported in customs data, 3/2022 – 12/2023 vs. 1/2021 – 2/2022. Comparison of G7-origin through G7-origin pre-invasion values to G7-origin through China values post-invasion.
[3] Average value per kilogram U.S.-origin Tier 1-4 items as reported in customs data, 3/2022 – 12/2023 vs. 1/2021 – 2/2022.

In the semiconductor context, the PRC is making every attempt to indigenize production of leading-edge chips. PRC leadership at the highest levels has focused on building an indigenous and self-sufficient semiconductor ecosystem, referring to integrated circuits in particular as critical to PRC national security strategy. Reporting from PRC state-owned media outlets has even referred to integrated circuits as the "main battlefield" of the PRC's MCF strategy. The PRC views its semiconductor dependence on the United States and U.S. allies as a major threat to PRC efforts towards military modernization, WMD development, and technologically-enabled human rights abuses.

We know semiconductors are the foundation of the world's economy – every device with an on/off switch has a semiconductor in it. In the national security context, though, it is the advanced compute integrated circuits that present the greatest threat to the United States, and our allies and partners. This is because those chips feed artificial intelligence (AI) capabilities.

U.S. and partner country semiconductor manufacturing equipment is used to manufacture advanced compute chips. Those chips are clustered together, enabling never-before seen advances in military capability. In fact, we know that the PRC is making investments in AI in weapons systems. Here is one example, based on publicly-available information:

- The PRC is reported to be the world's leading exporter of combat drones.
    - These military drones are reportedly used by the People's Liberation Army to patrol the PRC-India border, the Taiwan Strait, and Tibet. Earlier this year, they were reported to have deployed in the East China Sea, approaching Japan.
    - And the PRC is reportedly collaborating with Russian firms to advance the two countries' military drone technology.
- Now think of what is possible with drones enhanced by AI – AI built on the back of U.S. and partner semiconductor advanced chips or with advanced chips manufactured with U.S. and partner equipment.
- Most software is basically built out of if-then statements: if this, then that; if this, then that. For traditional software, you want chips that are good at taking many of these logical steps really fast, one after another.
- In contrast, an AI model works more like a human brain: it can take in rich inputs – audio and visual signals, for example – and make sense of them, and even recommend or take appropriate actions. AI chips can do many operations in parallel.
- Using AI-accelerator chips, those unmanned combat drones become autonomous. They can intelligently swarm independently, and navigate, select targets, and fire, without human instruction.
- Their lethality increases by leaps and bounds, and that lethality can be targeted precisely where the PLA and its partners are already deploying these systems.

This is just one example of AI-enhanced military modernization, which can be applied across all areas of military weapons systems – including hypersonic missiles, cyberweapons, and chemical, biological, radiological, and nuclear (CBRN) weapons of mass destruction – command and control, and logistics. The key developer of China's hypersonics program is publicly reported to have used a supercomputer to model and aid in military aircraft design; with more AI capacity would come more military capability. It's exactly what we're trying to forestall with our export controls.

Our goal from the beginning has been to protect our collective security by impeding the PRC's ability to indigenize the most advanced technologies, without unduly interfering with the continuing trade and development of technology.

Our response has been four iterations of controls on certain advanced computing items, supercomputers, and semiconductor manufacturing equipment. Because we started these actions in 2022, before ChatGPT and the hype around generative AI, we have had time to iterate on our approach and counter PRC attempts at diversion.

The update we announced yesterday adjusts our controls in several critical ways:

- We're adding new controls on many types of semiconductor manufacturing equipment, software tools for developing or producing semiconductors, and high-bandwidth memory (HBM), which is used in almost all AI data center chips.

- We're also making several changes that build on the effectiveness of our controls, including new red flag guidance that will work to address compliance and diversion concerns, and a significant number of Entity List additions that span PRC tool manufacturers, semiconductor fabs, and investment companies involved in executing the PRC government's furtherance of PRC military modernization.

This set of actions underscores the central role BIS has taken in this Administration for U.S. national security strategy – there is no Administration that has been tougher on the PRC, and that legacy will live on.

As a result of our controls, despite tens of billions of dollars in subsidies and a whole-of-government focus on semiconductor technology transfer, the PRC has only limited chipmaking capabilities at the 7nm node, which is itself more than 5 years behind the current leading edge.

As this technology gap continues to grow, the PRC will struggle increasingly to develop AI supercomputers capable of pushing the frontiers of weapons modeling, surveillance, and military modernization.

Cooperating with Allies and Partners

Through all of these measures, whether against the PRC or Russia, or any of the other myriad export control actions we've taken in this Administration, one thing is crystal clear: *we must work with our allies*. For the most part, the diligence this requires doesn't show up in our published regulations. We may put a photo of a meeting on our website here and there, but we don't tend to crow about the regularized efforts to ensure our allies and partners understand what we're doing and why we're doing it.

I have spoken extensively with foreign counterparts about the U.S. technology ecosystem and how they can align their export controls so that once our technology is exported, we have confidence it will be protected the same way it would be protected in the United States. When countries align their controls with ours, they reap the benefits of superior U.S. technology.

This isn't just theoretical.

In April, we updated our regulations to foster technological innovation with the UK and Australia, streamline defense and dual-use trade, and realize the goals of AUKUS, the security partnership with the United Kingdom and Australia. We: (1) removed license requirements for the export/reexport to the UK and Australia of a host of items including munitions, missile technology, and section engine technologies; (2) increased the availability

of license exceptions for reexport; and (3) removed restrictions on the export of high-speed and thermal imaging cameras to armed forces or for the production of military equipment.

In August, we published controls on quantum computing, with a carveout for countries that have similar controls, including Canada, Denmark, France, Finland, Germany, Japan, Netherlands, Spain, and the UK, and we understand that additional countries will follow suit. This action strengthens our trade and diplomatic relationships with like-minded countries and ensures that U.S. export controls keep pace with rapidly advancing technologies that pose serious threats to our national security when in the wrong hands.

In October, we provided additional license-free treatment for certain space-related exports to the UK and other allied countries. Specifically, we no longer require a license for the export of certain remote sensing or space-based logistics, assembly, and servicing satellites/spacecraft to some of our closest allies.

I previously mentioned our Global Export Control Coalition – I can't help but mention it again here as a glaring success story of countries coming together, driven by shared a national security perspective, to take coordinated and direct action to impede Russia from using U.S. technology on the battlefield in Ukraine.

Finally, we're working to apply these principles in the AI context, as well. In September, we expanded our Validated End User (VEU) program to include AI data centers. This action moves us in the same direction as our allies, in a way that pulls in individual companies. Our update contributes to the development of a trusted ecosystem for the responsible use of AI – an element of the Biden-Harris Administration's broader strategy to ensure the United States leads the way in responsible AI innovation and development. When companies demonstrate that they have high standards for physical security and cybersecurity measures, they unlock predictable and reliable flows of controlled data center technology.

Technology moves fast, and sometimes our governments are slow in our response. By creating trusted technology ecosystems through these examples, we create an environment with our allies and partners in which we have confidence that they will ensure our dual-use technologies are used in an aligned manner.

Only in collaboration with our allies can we address today's technology proliferation threats.

Conclusion

Our actions set the next Administration up to conduct sophisticated assessment of technology-based national security threats, and to take on strategic and targeted actions to protect our national security, together with our allies.

Dual-use export controls work has never been more timely, more relevant, or more effective, and our relationships have never been stronger. I am extraordinarily proud of our export control accomplishments, and want to close by expressing my thanks to all of my partners in this endeavor: the unparalleled team in BIS's Export Administration, whose hard work and passionate commitment to export controls make all of these efforts possible; Biden-Harris Administration leadership, especially Commerce Secretary Gina Raimondo, for their focus on export controls as a primary tool in national security policy; the foreign government counterparts who are deeply engaged in using export controls to enhance global peace and security; and the private sector actors who recognize their role on the front lines of export control compliance and enable the effectiveness of our regulations.

Thank you and I welcome your questions.