Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod to the Society for International Affairs 2022 Fall Advanced Conference
November 14, 2022

Thank you, Tom, for the generous introduction. And thank you to the Society for International Affairs for hosting me again today. A lot has changed since I last spoke with you in May. As just one example, last time I had to speak with you all remotely. I'm glad that today we can all be together in person.

Back in 1927, a man named Edwin Link invented the flight simulator. The story of Link, a New Yorker who fell in love with flying, is recounted in Daniel Coyle's book, "The Talent Code." In 1927, flying was an incredibly dangerous activity, where fatality rates at some Army aviation schools approached 25%. The belief was that good pilots were born, not made. That is, if you could survive a few hours in the air doing rolls and spins without throwing up, you were assumed to be capable of piloting an airplane, in need of only minimal additional ground training.

Link thought that there must be a better way to train pilots. And so, displaying his own brand of American ingenuity, he developed the first flight simulator. Roughly the size and shape of a bathtub, Link's technology allowed pilots to learn to fly in half of the time, at a fraction of the cost, with sharply reduced fatality rates. Eventually, the U.S. military took notice, and, by the end of World War II, a half-million airmen had logged hours in Link's simulator. You would think that this critical technology – which could give the U.S. military a distinct advantage in a dogfight – would be restricted from sale to nations adverse to the United States. But instead, hundreds of Link's devices were permitted to be exported to Japan, Germany, and the USSR in the years leading up to World War II.

One piece of technology – like a flight simulator – can be a military game-changer for a country, especially if it helps to provide overmatch. That's even more true today, where the power of technology, and its ability to provide overmatch, is exponentially greater than it was in 1927. As National Security Advisor Jake Sullivan recently highlighted, a fundamental connection now exists between our country's scientific and technological advantages, on the one hand, and our national security on the other. Our job at the Bureau of Industry and Security is to help preserve our country's scientific and technological advantages and thereby help protect our national security.

* * *

Last 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. It provides a roadmap for how we will work to advance our vital interests and pursue a free, open, and secure world.

As the Strategy makes clear, our two greatest priorities are out-competing China and constraining Russia. So-called "traditional" national security threats – like arms control and terrorism – remain pressing. We are focused on all these challenges, but today I want to focus on those two nation-state actors.

Since Russia further invaded Ukraine on February 24, we've used export controls to degrade Russia's military capabilities. Putin's war machine has been denied the critical supplies and spare parts it needs to replace its battlefield losses. We've built a coalition with 37 other countries to put in place the most expansive export controls in history aimed at a specific country. And they're working. Global exports of semiconductors to Russia, for example, have seen a sustained decline of approximately 70 percent since the invasion began, leaving Russian companies without the chips they need for weapons like precision guided missiles, unmanned aerial vehicles, and tanks.

The Russian military has been forced to rely on contraband chips, workarounds, and lower quality imports, which has undermined the effectiveness of their weapons systems. The Russian military is reportedly cannibalizing chips from dishwashers and refrigerators to fix their military hardware. They've taken Soviet-era tanks out of storage. They've also turned to third party countries – like North Korea and Iran – for supplies and equipment. Russian hypersonic ballistic missile production has nearly ceased due to a lack of chips. And a critical shortage of bearings has undermined their production of tanks, aircraft, submarines, and other military systems.

A critical part of this success has been both U.S. and international industry, with whom we have partnered to ensure that our controls are effective. Our agents have reached out to more than 600 domestic companies with past export ties to Russia or whose components have been identified inside Russian weapons systems found in Ukraine. And we've educated hundreds of international companies as well, through webinars and trainings.

We have also been active on the enforcement front. We've issued Temporary Denial Orders (TDOs) against ten Russian and Belarussian airlines – including Aeroflot, Russia's flag carrier – that were flying airplanes subject to U.S. law into Russia and Belarus in violation of our rules. These airlines are now prohibited from receiving U.S. parts for their airplanes. Over time, Aeroflot, Utair, Azur Air, and the others will be unable to continue flying, either internationally or domestically, as they are now cut-off from the international support, and U.S. parts and related services, they need to maintain and support their fleets.

And we've been paying attention to individual airplanes as well. We've publicly listed 183 aircraft that have flown into Russia and Belarus in apparent violation of our rules. In September, we also took action against four Iranian cargo planes, one of which contracts with the Iranian Air Force, that had been shipping electronics and spare parts to

Russia without our authorization. And last week, I reupped our TDO against Mahan Air, which in addition to supporting Iran's Islamic Revolutionary Guards Corps, has ferried materiel to Russia. The world is now on notice that any action related to these planes – including refueling, maintenance, repair, or the provision of spare parts and services – is subject to General Prohibition Ten of our rules.

More broadly, we have a significant number of ongoing investigations related to Russia. Just last month, for example, the Department of Justice unsealed an indictment charging individuals and companies in Europe with violating U.S. export laws by attempting to smuggle a jig grinder to Russia. Luckily, the jig grinder – a high-precision grinding machine system with potential application in nuclear proliferation and defense programs – was intercepted by law enforcement before it reached its destination.

* * *

In addition to constraining Russia, the National Security Strategy makes clear that we must out-compete China. Our national security requires that we prevent the PRC from misusing advanced U.S. technology. That's where we come in.

On October 7, BIS announced new rules to prevent the PRC from acquiring and using advanced U.S. technology to support China's military modernization. We had already imposed restrictions on exports to companies involved in China's military supercomputing and quantum computing efforts. These new rules, however, are meant to establish a clear technical line connected to military applications.

The new controls do this in three ways: first, by limiting China's ability to acquire advanced integrated circuits that have been used in AI applications tied to military modernization or human rights abuses; second, by preventing China from leveraging certain U.S. technology to support its supercomputer program, which directly enables its WMD and

military modernization efforts; and, third, by preventing China from leveraging U.S. semiconductor manufacturing equipment to indigenously develop or produce advanced chips as part of its military-civil fusion program.

These new rules require companies to come to BIS for approval of transactions involving specific items and activities of concern. The interagency—Commerce, Defense, Energy, and State—will then review any license applications under a presumption of denial for PRC end users. And we in Export Enforcement will be hard at work enforcing the new rules through all resources at our disposal, including classified and open-source reporting, partnerships with U.S. companies, administrative and criminal investigations, and our global end-use check program.

* * *

My side of the house in Export Enforcement also had an announcement on October 7. We've changed our policy on how we respond to a host government that is preventing our ability to conduct end-use checks overseas.

We've found that foreign governments generally welcome our end-use checks, as they are eager to receive U.S. exports and participate freely in the global economy. When a foreign government prevents our attempts to conduct an end-use check for a sustained period of time, however, we are faced with the unacceptable risk that U.S.-origin goods or technology will be misused, given our inability to verify a company's compliance with our controls.

Accordingly, we announced on October 7 a new, two-step policy to address instances of foreign governments frustrating our end-use checks through sustained scheduling delays.

First, end-use checks must be scheduled and completed promptly. If 60 days pass without a requested check being conducted, we will

initiate the regulatory process to add the foreign company to the Unverified List (UVL). As was true even before our policy announcement, placement on the UVL triggers additional regulatory requirements on exports to the listed company and notifies U.S. industry of our inability to determine the company's legitimacy as a recipient of controlled exports. Until a successful end-use check is completed, we stop processing licenses for the company and impose pre-license checks on all subsequent license applications received for exports to it.

Second, once the foreign party is added to the UVL, another 60-day clock starts. If we are not able to successfully complete an end-use check within the second 60-day window, we will initiate the regulatory process to have the foreign party added to the Entity List.

The rule announced on October 7 added 31 entities to the UVL, all of whom – along with 50 other companies previously on the UVL – are now at risk of moving to the Entity List as soon as December 6 (which is 60 days from October 7) if we are unable to complete an end-use check by then**.** I want to point out that the October 7 rule also removed nine entities from the UVL based on their having had a successful end-use check completed. In other words, the Unverified List is not an automatic pipeline to the Entity List. We want to verify the *bona fides* of a company so that it can participate in the global economy. When a company's end-use check is successful, it comes off the UVL.

End-use checks are a critical component of U.S. national security. And when we're not able to do those checks because of non-cooperation from a host government or other factors, placement on our lists will follow.

* * *

In addition to our end-use check policy change, let me quickly recap some other significant policy changes we've made since I last spoke with you in May.

In June, I announced four significant changes to strengthen our administrative enforcement tools.

First, we're now using our existing authorities to ensure that the most serious administrative violations trigger commensurately serious penalties. If you invest in an export compliance program while your competitor flouts the rules to gain an economic advantage, we are going to aggressively impose penalties on your competitor to help ensure a level playing field.

Second, we have done away with "no admit, no deny" settlements. We want companies – and industry generally – to have the opportunity to learn from others and avoid repeating their mistakes. When we enter a resolution, the settling party gets significant credit, in the form of a reduced penalty. But to earn that reduced penalty, we now require an accompanying admission that the underlying factual conduct occurred. That way, others can have a clear sense of what the company or individual did that got them into trouble and can modify their own behavior accordingly.

Third, in administrative cases where the violations do not reflect serious national security harm, we have been entering settlement agreements that do not require monetary penalties. We have been resolving these cases by focusing on remediation – through the imposition of a suspended denial order with certain conditions, such as training and compliance requirements. For the cases that we've resolved so far, we've imposed a two-year suspended denial of export privileges and required that the entities undergo compliance training. In one case, we also required an internal audit of the company's export controls compliance program.

Fourth, we amended how we process Voluntary Self-Disclosures (VSDs). For those VSDs involving minor or technical infractions, we are now resolving them on a "fast-track" with a warning letter or no-

action letter within 60 days of receipt of a final submission. For those VSDs that indicate potentially more serious violations, however, we are doing a deeper dive to determine whether enforcement action may be warranted, while at the same time adhering to the principle that companies deserve, and will get, significant credit for coming forward voluntarily. By fast-tracking the minor violations while assigning specific personnel to the potentially more serious ones, we are using our finite resources more effectively while also allowing companies that submit more minor VSDs to receive a quicker turnaround. For those wondering if our new process has "chilled" the submission of VSDs – it hasn't. We've received 150 new disclosures since the policy change, approximately the same average number of disclosures received for the same time period in the preceding two years. Companies continue to recognize that it is always better to knock on our door before we knock on yours.

In June, we also made a regulatory change to make charging letters public. Since that change, we've published five charging letters, including one alleging that Roman Abramovich, a Russian oligarch, unlawfully flew his two private jets worth an estimated combined $400 million to Russia. Just last week, we published a charging letter alleging that WEBS Electronics Trading Company unlawfully reexported U.S.-origin telecommunications equipment to Iran and Syria. These charging letters give the export community – and the wider world – visibility into what types of violations we see occurring and what we're doing about them.

* * *

While much of our work is done in partnership with industry, industry isn't our only important partner. In June, I announced our "Academic Outreach Initiative," which is our effort to help educate universities about export controls, given that the domains of national security and academia are now increasingly interconnected. We need to protect our sensitive technologies, which often stem from research

conducted at our universities, and prevent them from being used against us by adversaries.

Here's what we've done so far. We identified twenty academic research institutions whose work gives them an elevated risk profile. This summer, 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, and we've assigned each one an individual special agent to work with them. In September, Under Secretary Estevez sent a letter to each prioritized university noting the importance of maintaining a strong compliance program to guard against the risk of unauthorized exports.

In October and November, we conducted a webinar for the twenty universities on how export controls apply in academic settings and on ways to identify the national security threats facing academic research institutions. In December, we will be providing additional training on how best to conduct open-source research to better vet potential partners. And early next year, we'll conduct a broader training on regulatory requirements, including fundamental research in academic settings. In short, we're committed to doing all that we can to both protect national security and maintain U.S. leadership in academic research and innovation.

* * *

There's one more thing we're working on that I want to share with you today. And that's the thinking we've been doing about our metrics – how we track our investigative and analytic efforts – so that we can evaluate how tight the fit is between our highest priorities and what we're spending most of our time on. China and Russia are key priorities for the U.S. government and for BIS. At Export Enforcement, we want to make sure that our finite enforcement resources are effectively matched against these significant national security challenges. To do that, we need to make sure we're measuring the right things.

We are certainly not alone in this attempt to get our measurements right. Almost all law enforcement agencies – including federal ones like the FBI, DEA, and HSI – have confronted the challenges of how best to measure outcomes. And, throughout the law enforcement community, metrics are continuing to evolve. For many years, the default was simply to count the numbers of arrests made, convictions obtained, and jail terms imposed. Arrests, convictions, and sentences are fairly easily tracked. And, in the past, they were frequently used as proxies for law enforcement "success." But just as the broader law enforcement community has begun to search for different metrics in an attempt to better and more accurately measure the impact of their actions, so too are we at Export Enforcement.

In some ways, it should be less complicated for us to come up with metrics for success than it is for our some of our sister law enforcement agencies. Unlike many other federal, state, or local agencies, we are not responsible for a broad swath of statutes or a widely divergent set of crimes. Instead, our mission is singular – to enforce the nation's export laws in order to prevent the most sensitive U.S. technologies from falling into the hands of our adversaries. But even with that laser focus, it can still be challenging to discern which measures are the right ones.

We're still settling on the best way to measure our impact. But, as a preliminary step, we have begun evaluating our enforcement leads and cases against three criteria: (1) the criticality of the technology, (2) the end users of most concern, and (3) the end uses of most concern. Our thinking is that by inventorying our work against these criteria, we can help ensure that our enforcement resources are focused on our highest national security priorities.

For the first criterion – the criticality of the technology – our primary focus is on technologies that could eventually lead to military overmatch by a foreign adversary. We work with licensing officers from across the Departments of Commerce, Defense, Energy, and State to determine the highest-priority items on the Commerce Control List, as

well as additional chokepoint technologies that countries or end users of concern are dependent on from the United States. We also evaluate our own enforcement leads and cases to identify technologies explicitly sought for military applications or that enable human rights abuses.

With regard to end users – the second criterion – we are focused on military, intelligence, and security organizations in countries like China, Russia, and Iran. In addition, we, along with Treasury and State, have identified other actors of heightened national security concern. We're focused on them as well.

Our final criterion looks at end uses – or, more concretely, misuses of dual-use technology for applications such as nuclear weapons, missiles, chemical and biological weapons, advanced conventional weapons, and human rights abuses.

While we're still refining the best way to measure our impact, we have started to use these three criteria and to inventory our existing caseload against them. So far, these new criteria and metrics have proved helpful, both in confirming that our caseload is broadly in line with our priorities and in identifying areas for further analysis.

* * *

Edwin Link's invention of the flight simulator changed the battlefield of World War II, as it gave U.S. airmen (and, unfortunately, also some Soviet, German, and Japanese ones) the training and foundational skills they needed to pilot an airplane effectively. Today's technology advances are even more powerfully game-changing. No longer do wars require pilots to conduct aerial surveillance and strike ground targets. As we're finding out in Ukraine, unmanned drones are the new frontier in aerial combat – at a fraction of the cost of a manned airplane. This is the modern-day version of Edwin Link's core belief – that, through technological advances, we can increase warfighting efficiency and effectiveness. It is also how technologically over-

matched adversaries will try to overcome our military superiority. That's why the fight to keep U.S. technology – from the next-generation flight simulator to the next generation AI chip – out of the hands of our adversaries has never been more important.

Thank you, again, to the Society for hosting me today. The work that you're doing is an important complement to the work that we're doing at BIS. Keeping sensitive American technology out of the wrong hands is a shared endeavor. All of us at BIS are committed to helping industry understand both the importance of trade controls and the mechanics of how to comply with them. I look forward to continuing the partnership between Export Enforcement and the trade community in the coming months and years as we work together to keep our country safe and secure.