FOR IMMEDIATE RELEASE
Sept. 28, 2023
www.bis.doc.gov

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

Remarks as Prepared for Delivery by Assistant Secretary for Export Enforcement Matthew S. Axelrod at the Federal Office for Economic Affairs and Export Control-Bureau of Industry and Security (BAFA-BIS) Export Control Forum

September 28, 2023

Sixty years ago, at the height of the Cold War, President John F. Kennedy famously spoke to a crowd of over 100,000 in West Berlin. At the time, West Berlin was a haven for democracy, for hope, and for freedom – hemmed in on all sides by the Soviet Union.

During his speech, President Kennedy declared, in his inimitable Boston Brahmin accent: Ich bin ein Berliner. I am a Berliner.

His message was straightforward and clear. In the face of repression by a ruthless autocracy, democracy and self-government will prevail. Together, we will stand for freedom.

While President Kennedy delivered this message back in 1963, it resonates still. Despite the Berlin Wall having fallen over thirty years ago, the fight between oppression and freedom continues. The world President Kennedy faced then – with rising tensions between democracies and autocracies amid an intensifying technological arms race – has stark echoes in our world today.

Advances in science and technology are poised to define the geopolitical landscape of the 21st century. Disruptive technologies like quantum computing, artificial intelligence, and hypersonics may eventually be powerful enough to deliver military overmatch, with the potential to alter the balance of power in the world. We need to work together, with like-minded partners and allies, to protect our sensitive technologies from being used by our adversaries to undermine our security, our rules-based governments, and our individual freedoms.

At no point in history have export controls been more central to our collective security than right now. To borrow another phrase from President Kennedy, "in an age where the instruments of war have far outpaced the instruments of peace," we need to ensure that those instruments – and

the technologies used to develop, build, and maintain them – are not used by our adversaries to advance their military capabilities or facilitate human rights abuses.

At the U.S. Department of Commerce, where I am the Assistant Secretary for Export Enforcement, our law enforcement agents and analysts are focused on a singularly important mission: keeping our country's most sensitive technologies out of the world's most dangerous hands. But no one country's export controls can succeed without like-minded partners around the globe – partners from both government and industry. That's why it's so important and timely for BAFA to be hosting this forum. And why I'm so glad to have the opportunity to share a few thoughts with all of you.

* * *

Today, wir sind alle Ukrainer. We are all Ukrainians.

Russia's brutal invasion of Ukraine has resulted in the deaths of thousands of Ukrainian men, women, and children. The Russian military has destroyed cities and towns, targeted schools, bombed hospitals, and relentlessly attacked critical infrastructure. Russia's war has unleashed the worst global energy crisis since the 1970s, pushed global grain prices to record highs, and displaced thousands of people from their homes.

Much of this damage has been inflicted by one-way attack drones, also known as unmanned aerial vehicles or UAVs, supplied by Iran. While the specific Iranian drones being used by the Russian military are not the most sophisticated models, they are both effective and deadly. The drones' navigation systems allow them to fly specific pre-programmed routes with the help of GPS technology. Once programmed, they are highly accurate. They go where the Russian military wants them to go.

In other words, when the attack drones hit Ukrainian schools, apartments, hospitals, and critical infrastructure, it's not because they missed their intended target. To the contrary. These civilian structures were the intended targets. The Russian military is deliberately targeting civilian buildings. And not just any civilian buildings – those where schoolchildren go to learn and where sick and elderly patients go to receive medical care.

Since Russia attacked Ukraine on February 24 of last year, the Global Export Control Coalition, or GECC, has used export controls to help degrade Russia's military capabilities. The Russian defense industrial base has critical dependencies on the West, from electronics to machine tools to aerospace technologies. The 39-government coalition, which includes both the United States and Germany, has put in place the most expansive export controls in history in order to deny Putin's war machine the critical supplies and spare parts it needs to replace its battlefield losses. Assistant Secretary Thea Kendler, who you heard from yesterday, was instrumental in bringing that coalition into existence and has been instrumental in its continued work.

The GECC's work has demonstrated that technology export controls can be more than just a preventative tool. If implemented in a way that is robust, durable, and comprehensive, export controls can be a strategic way to impose costs on adversaries, and over time degrade their battlefield capabilities.

Global exports of semiconductors to Russia, for example, have seen a sustained decline since the invasion began, leaving Russian companies scrambling to obtain the electronics they need for weapons like precision guided missiles, UAVs, 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.

As our collective controls have degraded their weapons stocks, Russia has turned to suppliers outside of the coalition. They've turned to pariah states – like North Korea and Iran – for attack drones, ammunition, and even airplane parts.

But it's not just North Korea and Iran aiding the Russian war machine. Recent reporting suggests that Russia is being supplied by the People's Republic of China (PRC) as well. A recent Telegraph investigation found that Russian defense firms have received thousands of shipments from the PRC since February 2022, including drones, helicopters, and aerospace technologies.

In addition, parts from Western countries are being diverted for use in Russian weapons. A recent Washington Post article catalogued the manufacturing process of attack drones within Russia, and the dependencies the Russian facility has on the West. According to the article, over ninety percent of the electronic components are produced from Western designs, including U.S. and European-branded chips. Other reporting on Russia's drone production identifies dependencies on German machine tools and cables, Canadian antennas, and Swiss microcontrollers. These items typically aren't being sourced directly from Western suppliers, but are instead being diverted through third countries like the PRC and the former Soviet republics.

In response, Western countries are taking action. In March, German enforcement officials arrested a German-Russian dual citizen on multiple counts of violating the Foreign Trade Act by exporting electronic components to a company in Russia involved in the production of military materiel and accessories. In order to circumvent EU sanctions, the defendant is alleged to have imported electronic components from abroad to Germany, and then exported those same products to a company in Russia that manufactures the Orlan-10 drone.

In the United States, we've taken numerous enforcement actions against those alleged to have violated our Russia controls. This past July, for example, a suspected Russian intelligence operative was extradited from Estonia to face charges in the United States for providing American-made electronics and ammunition to the Russian military. More recently, at the end of last month, the U.S. Departments of Commerce and Justice jointly announced the arrest in Cyprus of Arthur Petrov, a dual-Russian-German citizen, for diversion of microelectronics to

Russian military manufacturers. At the same time, I imposed a Temporary Denial Order (TDO) against Petrov and six affiliated companies and co-conspirators for aiding this illegal scheme. And, just last week, we and DOJ jointly announced the unsealing of a complaint charging a Russian national, Maxim Marchenko, with running an illicit procurement network in Russia, Hong Kong, and elsewhere. As alleged, the procurement network fraudulently obtained large quantities of sensitive dual-use, military-grade microelectronics from U.S. distributors for Russian end-users. The network allegedly used shell companies and pass-throughs to transship the microelectronics to Russia through third countries, including Hong Kong and China. These microelectronics that Marchenko and his co-conspirators are alleged to have fraudulently procured have significant military applications, such as in rifle scopes, night-vision googles, thermal optics, and other weapons systems.

But beyond individual enforcement actions by individual countries, we need a coordinated international effort to prevent Russia from getting the materiel it needs to wage its brutal and unjust war. That effort must be twofold, comprising both a coordinated enforcement approach by allied governments and a robust partnership with industry.

* * *

On the government side, it's essential that we work together to ensure aggressive and coordinated enforcement. The work the GECC has done to date to successfully impose parallel controls is a testament to the importance of partnership. Now, though, we must work to make sure that we are similarly coordinated in implementing and enforcing those controls.

It is helpful that we share the same objectives as our partners at BAFA, namely that exports should neither reinforce conflicts nor contribute to internal repression or other significant human rights violations. And we have a long-standing working relationship with our other German government colleagues, including the Ministry of Economy and the Customs Investigation Bureau (ZKA), through our Export Control Officers (ECOs) stationed right here in Frankfurt, who help ensure that our controlled technology and goods are safeguarded from diversion.

More broadly, in April, our Deputy Secretary, Don Graves, along with his counterparts from the U.S. Treasury Department and the Japanese Finance Ministry, convened a meeting of the G7 countries to announce a new enforcement coordination mechanism. The goal is to bolster coordinated international enforcement of the Russia controls among Canada, France, Italy, Japan, the United Kingdom, the European Commission, the U.S. and of course Germany. Just last week, we hosted the first meeting of the G7 sub-working group on export enforcement, where we analyzed Russian evasion strategies, shared information on diversion through third countries, and discussed best practices for compliance and enforcement, including coordinated outreach to industry. My participation here today is reflective of this important effort and our close working relationship with our G7 colleagues.

Additionally, in June, I was in Ottawa meeting with government representatives from Canada, the United Kingdom, Australia, and New Zealand. We announced a commitment to formally coordinate on export control enforcement. Similar to our G7 effort, we agreed to increase collaboration and information sharing across our respective enforcement teams to address evasion of export controls. We have since decided to use the nickname "E5" to refer to the group of countries engaged in this coordination effort.

We have also expanded our international footprint to collaborate with governments across the globe. We now have 11 Export Control Officers and one enforcement analyst stationed in 10 locations outside the United States. In July, we established a new Export Control Officer presence in Taiwan. And, last month a new Export Control Officer began work in Helsinki. In addition, for the first time ever, we have stationed an enforcement analyst outside the United States. We now have a BIS analyst assigned to Ottawa to liaise on export controls directly and daily with the Canada Border Services Agency and our other Canadian partners.

We are mindful, however, that working among likeminded coalition partners alone isn't sufficient to address the issue of illicit transshipment. Assistant Secretary Kendler and I, along with our U.S., EU, and UK partners, have been traveling to numerous non-GECC countries to inform our government counterparts of our concerns and the consequences of continued diversion. As one example, I traveled to Kazakhstan and Kyrgyzstan this past summer with colleagues from the Department of the Treasury, as well as the sanctions coordinators from the UK and the EU, to talk to the Kazakh and Kyrgyz governments about evasion of our Russia controls.

I also recently visited Beijing with U.S. Commerce Secretary Gina Raimondo where she and her counterpart from China's Ministry of Commerce launched an export control enforcement information exchange, one that will allow us to communicate directly about the need for compliance with our rules and the actions we will take when those rules are violated. My Chinese counterpart and I held the first in-person meeting of the information exchange at the Ministry of Commerce in Beijing. Among other things, I conveyed our strong concerns about Chinese companies violating our Russia controls by transshipping U.S. items through the PRC to Russia. I also could not have been clearer about the consequences that such actions will trigger.

* * *

So that's some of what we've been doing at the government-to-government level. But nothing is more important than the actions you in industry can take. You are our first line of defense. You know your industry best. You are the ones receiving the orders, the ones who will first spot any red flags. No one knows your business, and the export control risks inherent in it, like you do. So, what am I asking of you?

I'm asking you to partner with us in this fight. I'm confident my German enforcement colleagues would agree with me when I say that we would much rather work with companies to

prevent export violations on the front end than enforce violations on the back end. When we enforce, it typically means the technology has already gone to our adversaries and the national security harm has already occurred. Our collective goal is to avoid getting to that point whenever possible.

As government enforcers, it is a priority for us to talk with you about how our export controls work and to help you sharpen your compliance efforts. The last thing you want is for your product to be recovered on the battlefield in Ukraine, for your product to play a role in the death of a Ukrainian civilian or soldier. And that's the last thing we want too.

Since the Russia controls went into effect, our agents have reached out to more than 800 U.S. 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, including those coordinated by our Export Control Officers here in Frankfurt.

Given the increased scope of our Russia controls, especially for items not traditionally controlled by the multilateral export control regimes, we recognize that we need to prioritize our asks of industry. Earlier this year, the U.S., EU, Japan, and UK identified specific technology dependencies that Russia has for its military operations. Accordingly, we initially identified 38 Harmonized System or HS codes tied to these technologies, and we recently expanded it to 45 HS codes earlier this month.

Within those 45 HS codes, we in the U.S. are most highly focused on the nine codes representing the most important items for Russia's and Iran's missile and UAV programs. As discussed earlier, Russia is using Western parts to help power weapons used to constrain Ukraine's military operations and sow terror through the targeting of civilian infrastructure and homes. We're asking industry to focus specifically on transshipment and diversion of these battlefield items. And while our efforts in the U.S. have focused primarily on the nine codes – because they capture the majority of U.S. items that are being used by the Russians to wage war – companies outside the U.S. are shipping other key items that are chokepoints for Russia's war machine. That's why we've prioritized the nine codes in the U.S., but as part of the longer list of 45. If your company sells items falling within any of the 45 HS codes, you should be extra vigilant to ensure those items aren't being diverted through third countries to Russia.

I'm hopeful this isn't the first time you've heard that we're focused on these HS codes. We've taken a number of actions to spread the word and build awareness, particularly about the top nine.

First, we issued guidance to industry. In June 2022, in partnership with our country's Financial Crimes Enforcement Network (FinCEN), we issued a joint alert to financial institutions. The alert described red flags for financial institutions to look out for to help prevent items from being diverted. Importantly, the alert created a unique key term for financial institutions to use when

filing Suspicious Activity Reports (SARs) related to Russia diversion, and I'm pleased to say that in just the first 15 months of its operation, we have received over 400 filings. We've been able to action nearly one-third of those SARs in various ways, including by cutting leads to our enforcement agents, advancing existing cases, and developing Entity List packages.

In May 2023, we issued a second joint alert with FinCEN and a separate tailored product for exporters that specifically highlight the nine HS codes as well as tactics that Russia is using in attempts to evade our controls. We identified three fact patterns for exporters to be wary of, as they are indicative of possible attempted circumvention of our controls: (1) the customer never received exports prior to February 24, 2022, the date of the Russian invasion, but is now ordering items falling into one or more of the nine HS codes; (2) the customer received U.S. exports prior to the start of the war, but those exports did not fall into one or more of the nine HS codes and now do (like a beauty salon that has recently started importing microelectronics); and (3) the customer received U.S. exports of items within the nine HS codes prior to February 24, 2022, but has since significantly increased their order volume. If you see any of these fact patterns, we ask that you do extra due diligence. Don't sell to customers who are helping to fuel the Russian war machine.

In June, we did a first-ever quad-seal advisory along with our country's Departments of Justice, Treasury, and State to alert industry about the threat of Iran's drone program and to highlight effective due diligence policies, compliance structures, and internal controls that can be employed to harden supply chains against the threat posed by illicit Iranian UAV procurement efforts.

And just earlier this week, through our E5 partnership, we published an advisory for industry, co-authored by all five countries' governments. This is the first "quint-seal" advisory of its kind. This new advisory again amplifies the importance of the high-priority items that Russia is using in its weapons systems, as well as the need to apply a risk-based approach to export compliance.

All of these guidance documents are available on our website and I encourage you to review them.

Second, we've been reaching out to U.S. companies, like electronics distributors and trade associations, to educate them on the problem of Western parts ending up in Russian missiles and drones. We've identified specific customers of those companies that meet one of the fact patterns I just described and notified companies about them. This information should result in companies conducting enhanced due diligence on their customers before filling orders, and we have already been informed of a number of order cancellations to prevent diversion.

Third, we worked with our colleagues from Export Administration to impose license requirements on third parties, either by individually informing companies of these requirements, or by adding parties to the Entity List. Just earlier this week, in fact, we put 28 more parties on the list, including a number for their role in procuring components for Iranian and Russian

UAVs. To date, BIS has added over 600 parties to the Entity List for supporting Russia's military – including more than 60 in third countries like China and Iran for seeking to supply Russia's military after implementation of the new controls. If you ever have a question about whether one of your potential customers is on the Entity List or another U.S. restricted party list, you should check our Consolidated Screening List, available for free on our Commerce Department website.

Fourth, we have initiated investigations and brought criminal charges. Our cases, like the Petrov indictment and TDO and the Marchenko complaint I mentioned earlier, help bring accountability to those who we believe have violated our rules by sending battlefield items to Russia. Our cases also help ensure that those who expend the resources to implement effective compliance programs are not placed at a competitive disadvantage.

That's a lot of work so far. But we're not close to done. Among other things, we're working to further amplify our industry efforts internationally. We have been consulting with GECC partners on identifying additional red flags and on establishing best practices for coordinating with industry across the coalition. By making coordinated approaches to industry in partner countries, we seek to put everyone on an even playing field with comparable due diligence expectations.

I also have two specific requests of you to help prevent diversion of your products, particularly those ending up on the battlefield. First, if you don't already have one, you need to institute a strong export compliance program as a critical component of your overall corporate compliance structure. Having such a program in place protects both your company by mitigating risk, as well as our collective security by keeping sensitive technology out of the wrong hands. BAFA's published guidance on compliance programs states that "it is in the power of the companies themselves to make their contribution to detecting procurement attempts early and preventing them by establishing suitable organizational measures and provisions." In other words, a robust internal compliance program is paramount.

Second, I ask that you implement end-user verification statements when you receive a customer order for items that fall into any of the priority HS codes. By asking for written certification of that customer's business history, the specific end use, and the specific end user of the exported item, you can better identify red flags and deter diversion. This is especially critical when dealing with customers in countries outside of the Global Export Control Coalition. Today, BIS is publishing "best practice" guidance for industry recommending the use of these customer certifications. Such a certification statement can help ensure that parties to the export transaction are, in essence, who they say they are, and that the goods are going where they should be. While our guidance is directed at U.S. industry, it can be instructive for industry everywhere. Together, we can harden our supply chains to prevent the diversion of goods that help prop up the Russian war machine.

* * *

While I'd venture to guess that "Ich bin ein Berliner" are the most famous words President Kennedy ever uttered in Germany, back home in the United States, there's a line of his that's even more well known. It comes from his inaugural address and highlights that, as citizens, we are not just given rights by our government but obligations as well. As President Kennedy put it, "[a]sk not what your country can do for you, but what you can do for your country." With these words, President Kennedy sought to inspire his fellow Americans, urging them to coalesce around a common goal of peace and security at the height of the Cold War.

What's not nearly as well remembered is the line that followed. His next line was a call to action not just for Americans, but for people across the globe: "My fellow citizens of the world: ask not what America will do for you, but what together we can do for the freedom of man."

In the United States, we've asked industry to partner with us to meet the urgent challenge of degrading Russia's ability to wage war against the Ukrainian people. We've asked them to redouble their compliance efforts, to watch out closely for red flags when exporting goods that can be used on the battlefield, and to be deeply skeptical of new customers ordering sensitive items in countries known for transshipment. I'm here to ask the same of you. You represent some of the largest, and most important, industries in Europe. And you can play a critical role in hindering Russia's ability to wage its illegal war in Ukraine.

None of us do this work alone. The work that you do is a crucial counterpart to the work that your governments are doing, that U.S. industry is doing, and that we're doing at BIS. Together, we can degrade Russia's battlefield supply of missiles, tanks, and drones. Together, we can help the Ukrainian people in their fight to defend their homeland against unprovoked Russian brutality. Together, we can work to ensure the continued "freedom of man."

Thank you.