FOR IMMEDIATE RELEASE
June 30, 2022
https://bis.doc.gov

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

Assistant Secretary for Export Enforcement Matthew S. Axelrod
BIS's 2022 Update Conference on Export Controls and Policy
June 30, 2022

Remarks As Prepared for Delivery

Thank you, Kevin, for that kind introduction. And, more importantly, thank you for all you have done over the past twenty-five years – and continue to do every day – to help BIS advance its mission and keep our country safe. And thank you to all of you for being here today, either in person or virtually. I am so excited to be here with you, speaking at my first Update Conference.

I've been in the seat since the beginning of January, so I'm now a grizzled six-month veteran of BIS. While I'm joking, there's actually a bit of truth to it. Six months may not sound like a long time, but Kevin tells me he'd put the past six months up against any six-month period in BIS's history. Sparked by Russia's brutal and unprovoked war against Ukraine, the pace and scope of changes to our export control rules are without precedent. And, given the global threat environment we currently face, our enforcement efforts have never been more central to America's national security strategy.

I want to take today as an opportunity to talk a little bit about what we at Export Enforcement, or EE, have accomplished in the past six months and then a little bit about what we have planned for the future. And when I say "what *we* have accomplished," I really mean the accomplishments of the incredible team of agents, analysts, and export compliance specialists I have the honor to lead. These men and women work tirelessly every day to deny our adversaries the sensitive technology they desire – technology our adversaries would then use in their quest to overcome the United States' military superiority. We may not be the biggest law enforcement agency, but no agency enforces export controls – or antiboycott controls for that matter – better than EE.

As you all know, Russia launched its invasion of Ukraine on February 24th. That same day, the United States and our partner countries put in place the initial wave of what would become the most expansive export controls in history aimed at a specific country. Since that day, both the scope of the restrictions put in place, and the number of countries standing shoulder to shoulder alongside us in this effort, have only continued to grow. Thanks to the incredible work of Thea Kendler, Matt Borman, and their team, BIS has issued 12 separate rules aimed at degrading Russia's ability to continue to wage war against the people of Ukraine, rules that have been complemented by parallel actions taken by our now 37 coalition partners.

EE's enforcement of these enhanced Russian export controls has been swift and powerful. Our agents have detained or seized over 200 shipments valued at over $88 million. I have signed nine temporary denial orders, or TDOs – including three that I signed last Friday – against Russian and Belarusian airlines; those orders should ground significant numbers of Russian- and Belarusian-operated planes. We've also, for the first time ever, published lists of airplanes we believe have violated our controls. We did that to put the world on notice that providing services or parts to those planes will place the providers in violation of General Prohibition 10 of the EAR. And while these TDOs and our General Prohibition10 list have successfully hampered Russian owners' abilities to fly these aircraft, we've also been busy granting case-by-case authorizations to return specific planes to their Western owners, thereby helping to thwart Vladimir Putin's efforts to steal American and European assets.

On June 6, OEE administratively charged oligarch Roman Abramovich for illegally exporting his Gulfstream 650 and 787 Dreamliner, planes worth an estimated combined $400 million. On the same day, the Department of Justice, with OEE's assistance, obtained seizure warrants for the two planes. The public nature of the OEE charging letter represents the first use of an important regulatory change that just became effective on June 2nd – our charging letters will now be public when issued, rather than down the road after a matter is resolved. Prior to the change, the public wouldn't know when a charging letter was issued, and there wasn't as strong an incentive for those under investigation to try to resolve matters quickly. And because the wider world wasn't given visibility into what types of violations we saw occurring until those violations were later resolved, other companies sometimes didn't have the information they needed – information that would have sparked urgency to upgrade their compliance program or to submit a voluntary disclosure. To address those issues, we made a change. Now, charging letters are public when filed with the Administrative Law Judge. Once that happens, we put them up on our website for public viewing. That's not to say we'll always go straight to a charging letter. In appropriate cases, we will still use pre-charging letters, which are not public, and which allow us to give a company notice of what we think they've done wrong. In appropriate cases, pre-charging letters can be a useful tool as they allow us to have conversations and negotiations about a resolution prior to a charging letter being issued publicly.

We've been innovative in other ways as well. Two days ago, on Tuesday, we partnered with the Treasury Department to issue the first ever joint BIS-FinCEN alert. This unprecedented joint alert informs financial institutions about the specifics of our new Russia controls and identifies red flags that those institutions should be looking for as indicators of potential evasion. The joint alert also gives financial institutions a specific code to use in their Suspicious Activity Reports when they identify transactions they think might be designed to evade the controls. The use of this special code will in turn allow our investigators to review SARs for potential violations of the Russia controls more quickly and should help lead to enforcement actions.

We want our investigators to have powerful tools to identify violations because once identified, we can take action. Take, for example, the Entity List announcement this week identifying eight companies for backfilling – in other words, for shipping items to Russia to replace the items Russia is no longer able to obtain from the United States due to the enhanced controls. Identifying these parties came about because of the terrific research our enforcement analysts, working with interagency partners, were able to do. Secretary Raimondo has been

crystal clear that we will not tolerate parties in third countries undermining our export controls, and Tuesday's announcement delivers on this promise. These listings are in addition to almost 300 Russian and Belarusian defense sector companies we have added to the Entity List since Russia's invasion of Ukraine.

Our enforcement efforts have not been limited to Russia alone, of course. While the invasion of Ukraine has rightfully occupied a lot of our time, we have also been laser focused on identifying violations tied to China. CIA Director Burns has identified China as "the most important geopolitical threat we face in the 21st Century." The PRC is determined to advance China's military capabilities by illicitly acquiring U.S. technology. Our job is to prevent them from doing so.

The Temporary Denial Order I issued on June 8th is an example of our efforts. Our investigation uncovered a scheme by three interrelated companies – Quicksilver Manufacturing Inc., Rapid Cut LLC, and U.S. Prototype Inc – that contracted with U.S. defense and aerospace customers to 3-D print items based off sensitive prototype space and defense technologies. Unbeknownst to their customers, the three companies sent the blueprints and technical drawings to China, without the required export licenses, to have the items 3-D printed there and then shipped back to the United States. In response, we imposed what some consider our most powerful administrative tool – the denial of export privileges. And while the investigation continues, those companies will no longer be able to ship sensitive U.S. technology to China, risking that technology falling into the hands of the PRC.

We have been using other administrative tools as well. In February, I added 33 Chinese parties to our Unverified List as a result of our inability to conduct end-use checks on them. When a requested end-use check cannot be performed, we cannot have confidence that items sent to that party will be used for their intended purpose. Until and unless we are able to conduct the checks successfully, those 33 parties will remain on our list.

Earlier this week, in addition to identifying eight Chinese parties on the Entity List for their backfilling to help Russia, we added 25 other Chinese parties for involvement in military modernization and Iran sanctions evasion activities. Those additions bring us to a total of over 100 Chinese parties added to the Entity List during the Biden Administration, for an overall current total of nearly 600 – nearly 600 Chinese parties that the interagency has determined to have been involved, or to have posed a significant risk of being involved, in activities contrary to the national security or foreign policy interests of the United States. That number includes parties leveraging artificial intelligence applications to support the Chinese Police's subjugation of Uyghur Muslims in Xinjiang; of quantum technology acquisitions by China for WMD and military modernization purposes; and efforts to leverage semiconductor designs for high performance computers that can model Chinese hypersonic missiles.

Beyond enforcement actions involving Russian, Chinese, or other actors, we have also been busy building coalitions – with industry, with academia, and with foreign partners.

For industry, we have just finished revising our *Don't Let This Happen to You* guidance document, which provides examples of what happens when individuals or companies don't

comply with our regulations. In fact, we just uploaded the new version to our website today, so industry will have an up-to-date compendium of examples to help drive compliance. Separately, we've been working hard to educate the exporting community about the Russia controls – our philosophy being that we'd rather deter violations on the front end than enforce on the back end after a violation has occurred. Our Export Control Officers stationed overseas have organized seminars with U.S. and international business associations to explain the new Russia controls, with more than 1,500 companies trained to date. And, domestically, our agents have visited more than 500 U.S. companies with a history of exporting to Russia to explain the new rules and to partner on preventing diversion.

Having our agents spread across the country allows us to better know the exporting community, and the technologies being exported, so that we can help protect them from unauthorized use. In that regard, I am pleased to be able to announce that, thanks to the President and to Congress, our footprint is growing. The Office of Export Enforcement is located in 30 cities nationwide, and today I am announcing that our Phoenix location will officially become our ninth full Field Office. Given the region's growing semiconductor manufacturing presence, and the important role this technology plays for our U.S. national security, we're excited to be able to bring a full complement of agents there.

For academia, I was in Pittsburgh on Tuesday to announce our "Academic Outreach Initiative," which is the name of our new effort to help educate universities about export controls and their importance to national security. Our research universities are an essential component of the scientific and technological success that powers the engine of the American economy. But they can also sometimes present an inviting target for foreign adversaries. Our goal is to help these institutions maintain their open collaborative research environments in a way that allows them to protect themselves from national security risk. The Initiative has four elements. First, we're prioritizing engagement with academic research institutions whose work has resulted in an elevated risk profile – for example, those universities that are engaged in sensitive research for the Department of Defense or have ties to parties on the Entity List. Second, for each prioritized university, we're designating a specific local Special Agent to serve as a dedicated point-of-contact who will offer to hold regular meetings with them. Third, we'll be offering background briefings for prioritized universities on known national security threats. And, fourth, we will be training universities on how to comply with EAR license requirements and implement an Export Management and Compliance Program, as well as on how to vet potential foreign partners to determine connections to parties that are on the Entity List or otherwise of concern. By launching this initiative, we hope to work alongside our great research universities to protect the innovation driven by professors and students of all nationalities from illicit acquisition attempts by foreign governments.

At the government-to-government level, the Department of Commerce has been leading an effort to establish international enforcement partnerships and coordination mechanisms. Earlier this month, Deputy Secretary Don Graves and I met with European Commission counterparts to lay the groundwork for an U.S.-EU enforcement cooperation strategy, and the following week, I met virtually with counterparts from Canada to publicly announce a strengthened partnership between Export Enforcement and the Canada Border Services Agency.

These efforts are already producing results, including through surges in end-use checks and coordinated detentions and investigations with our partners in Canada and Europe.

Thanks to President Biden and to Congress, we were provided with supplemental resources to expand our international partnerships by deploying additional Export Control Officers. We've started by implementing long-term deployments, including at the U.S. Embassy in Helsinki and the American Institute of Taiwan in Taipei. And, in May, we deployed our first intelligence analyst abroad. We now have an analyst working side-by-side with the Canada Border Services Agency to identify illicit reexports through Canada and to speak with Canadian companies about export compliance.

So that's what we've been up to so far this year. You can see why I say it's been such a busy six months. Now let me talk about what comes next.

It's my view that our enforcement tools have never been a better match for the global threat environment than they are right now. Given that, we need to make sure we are using those tools to their fullest potential. In partnership with our Office of Chief Counsel, we are going to focus our greatest attention on the most serious violations, by prioritizing the cases that do the most harm to our national security. That way, we can ensure that we use our finite resources to maximum effect.

Today, I am announcing four policy changes to help accomplish this prioritization strategy and strengthen the power of our administrative enforcement tools. These four changes are laid out in a policy memorandum that I issued earlier today to the entire EE workforce and that will be publicly available on our newly revamped enforcement website.

First, we will use all of our existing regulatory and statutory authorities to ensure that the most serious administrative violations trigger commensurately serious penalties. By aggressively and uniformly applying the existing BIS settlement guidelines, we will ensure that all appropriate cases are properly deemed "egregious," which opens the door to more significant penalties under our regulations. In addition, we will ensure that the existing aggravating penalty factors are applied more uniformly to escalate penalty amounts where appropriate, which parallels how mitigating factors are currently applied to reduce penalty amounts. In short, 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 create a level playing field. In addition, by imposing stiff penalties, we want to create a strong disincentive for those considering circumvention – one that hurts both the pocketbook and reputation of violators.

Second, in keeping with our goals of ensuring a level playing field and incentivizing investments in compliance, we are doing away with "no admit, no deny" settlements. We want companies – and industry generally – to have the opportunity to learn from others and avoid making the same 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, there needs to be an admission that the underlying factual conduct occurred. That way, others will have a clear sense

of what the company or individual did that got them into trouble and can modify their own behavior accordingly.

Third, to help clear through pending administrative cases where the violations do not reflect serious national security harm but do rise above the level of cases warranting a warning letter or no-action letter, we are going to offer settlement agreements that do not require monetary penalties. Instead, we will seek to resolve cases by focusing on remediation – through the imposition of a suspended denial order with certain conditions, such as training and compliance requirements. Any such resolution will be contingent on the violator's willingness to accept responsibility, admit to the conduct, and commit to enhanced compliance measures.

Fourth, we are amending how we process Voluntary Self-Disclosures (VSDs). For those VSDs involving minor or technical infractions, we will resolve 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 will do a deeper dive to determine what type of 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. The VSDs that are not fast-tracked will be assigned to a Special Agent and an OCC attorney. In the most serious cases, the Department of Justice's Counterintelligence and Export Controls Section will assign an attorney as well. (As an aside, please know that VSDs to us don't qualify you for benefits under DOJ's VSD program. As their policy makes clear, to qualify for their program, a company must disclose to DOJ also.) By fast-tracking the minor violations while assigning specific personnel to the potentially more serious ones, we will be able to use our finite resources more effectively while also allowing companies that submit more minor VSDs to receive a quicker turnaround.

These four changes are designed to enhance our administrative enforcement program and to help make it as effective as possible. While these changes will be applied within our existing regulatory framework, they do come on top of a fifth change made earlier this month that was regulatory in nature – a regulatory amendment making charging letters public. So that's where we are for now. Depending on how these collective changes play out, we may consider further ones as well. We are committed to making whatever changes are necessary to maximize the effectiveness of our administrative enforcement of export violations.

In addition to the export side, I also oversee the Office of Antiboycott Compliance, or OAC, which has administrative enforcement authority over our antiboycott laws. These laws prohibit U.S. persons from supporting unsanctioned foreign boycotts against countries friendly to the United States, such as the Arab League boycott of Israel. Because violations of the antiboycott regulations cause real harm to the principle of free trade and to our national security and foreign policy interests, strong enforcement and accountability measures are needed. To that end, we are reviewing ways to further enhance OAC's enforcement posture to reflect the seriousness with which we view antiboycott violations and to discourage U.S. companies, in the strongest possible terms, from cooperating with any unsanctioned boycott.

More specifically, we are considering revising the EAR to recategorize the relative seriousness of the various antiboycott violations to better comport with current boycott-related activity and with OAC's priorities and practices. In addition, we are evaluating current penalty levels to determine whether they should be higher – both to sanction those who violate the law and to deter those who would. And, last, like I announced today with regard to export cases, we're considering whether to eliminate "no admit, no deny" settlements in order to incentivize compliance and strengthen deterrence. I expect to have more to say about where we'll land on these questions in the coming weeks.

Thank you again for being here today and for your continued partnership in this effort. We at BIS don't do this work alone. All of you who make up the exporting community are on the frontlines alongside us. And just as your clients and companies rely on you to keep them in compliance and out of trouble, so do we. So, thank you for all you do to help ensure our rules are followed and our sensitive technology kept secure. If the last six months have taught us anything, it is that all of us must remain vigilant in protecting our democratic principles, our shared values, and our technology from misappropriation. Thank you.