FOR IMMEDIATE RELEASE
May 16, 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 DELIVERS REMARKS TO THE SOCIETY FOR INTERNATIONAL AFFAIRS 2022 SPRING VIRTUAL ADVANCED CONFERENCE ON EXPORT CONTROLS & INTERNATIONAL POLITICS

Monday, May 16, 2022

Remarks as Prepared for Delivery

Thank you, Marc, for that kind introduction. Thank you to the Society for International Affairs for hosting me today. And thank you to all of you for tuning in. I'm hopeful that virtual conferences will soon go the way of the 8-track (and, as of last week, the iPod) and we can safely gather in person once again in the near future.

This year marks the 40th anniversary of the Office of Export Enforcement, which – thanks to President Biden, Secretary Raimondo, and the United States Senate, I now have the honor to oversee. For forty years, special agents from OEE have been on the frontlines, ensuring that sensitive U.S. goods and technologies aren't falling into the wrong hands abroad. Their efforts, and their results, have been constants for those forty years. But the nature of the goods and technologies themselves, and their relevance to the primary national security threats facing our country, have shifted dramatically during that time span.

Forty years ago, our export control system was narrower, focused singularly on traditional dual-use items related to conventional military applications, and were aimed a single adversary. The Coordinating Committee for Multilateral Export Controls, or CoCom, was established by the United States and our allies after World War II as an informal mechanism to coordinate an embargo policy on the export of sensitive technology and goods to the Communist bloc. CoCom gave a veto to the United States or a participating ally over the export of any multilaterally-controlled item destined to the Soviet Union or a Warsaw Pact country. This arrangement prevented the backfilling of exports when one allied country denied an export, squarely preventing Russia from acquiring advanced technologies to support its Cold War ambitions. In 1982, when the Office of Export Enforcement began, it's job was to enforce United States export control laws in a CoCom world.

From these narrow post-World War II beginnings, the global export control system evolved in the mid-1990s with the simultaneous fall of the Soviet Union and rise of the proliferation of weapons of mass destruction. The single mechanism of CoCom gave way to multiple export control regimes focused on a broader array of items – not only dual-use items

tied to conventional weapons, but also items related to missiles, chemical and biological weapons, and nuclear weapons. This structure posed unique challenges, however, because of splintered agreement among allies about how to treat countries like Russia, China, and Iran. If Russia, for example, could simply obtain advanced technologies from Europe that the U.S. denied, the ability to impede their military's technological advancement was undermined – while U.S. industry lost business to their European competitors.

Fast-forward twenty years to 2002 and the focus of our country's national security efforts had recently pivoted to face a new and pressing threat – that of terrorist attacks on our homeland by non-state actors like al-Qaeda. In the years following 9/11, our government surged resources to meet this threat, with significant success at preventing follow-on attacks. For OEE, the changing nature of the threat meant that in addition to investigating the proliferation of WMD and destabilizing military activities, we also worked more closely with the Department of Defense to prevent U.S. components from getting into the hands of terrorists for use in improvised explosive devices. And, in parallel, we expanded the use of our Entity List to allow for the designation of parties when supporting any activity contrary to U.S. national security or foreign policy interests.

Today, forty years since OEE's founding and a little more than twenty years since 9/11, the national security landscape has changed yet again. While non-state actor threats of course remain, experts assess that nation-state actors are now the paramount threat. Each year, the Office of the Director of National Intelligence publishes the Intelligence Community's Annual Threat Assessment, which details the IC's view of the gravest national security threats faced by the United States. The differences between the first such assessment, issued in 2006, and this year's assessment are striking. In 2006, the DNI stated on the assessment's very first page that "terrorism is the preeminent threat to our citizens, Homeland, interests, and friends." The 2006 assessment's first section is on the "Global Jihadist Threat," followed by a section on "Extremism and Challenges to Effective Governance and Legitimacy in Iraq and Afghanistan." Analysis of the threat posed by Russia does not appear until page 16, with the China discussion not appearing until page 20.

Compare that to this year's assessment and you will see how significantly our national security landscape has changed since 2006. The first four sections of this year's assessment each focus on a different nation-state actor – China, then Russia, then Iran, then North Korea. As the assessment notes on its first page, "Beijing, Moscow, Tehran, and Pyongyang have demonstrated the capability and intent to advance their interests at the expense of the United States and its allies." The assessment later goes on to point out that "China will continue pursuing its goal of building a world-class military that will enable it to secure what it views as its sovereign territory, establish its preeminence in regional affairs, and project power globally while offsetting perceived U.S. military superiority," will "continue the largest ever nuclear force expansion and arsenal diversification in its history," and "is working to match or exceed U.S. capabilities in space to gain the military, economic, and prestige benefits that Washington has accrued from space leadership."

Given that threat picture, I submit to you that the job of our Office of Export Enforcement agents – preventing sensitive U.S. technologies and goods from being used for

malign purposes by those would do us harm – has never been more important, never been more central, to the national security threats we face than at any other time during the organization's forty-year existence. It's among the reasons why I'm so honored to lead those agents, and the analysts who work in tandem with them, at this point in history. And it's why I feel such a strong sense of urgency about our work and how we go about doing it.

President Biden vividly captured this national threat picture in this year's State of the Union address, when he described the ongoing "battle between democracy and autocracy."

Today, we are tragically witnessing this battle play out in real time as Russia continues its brutal and unprovoked war against its peaceful, democratic neighbor, Ukraine.

As I'll discuss, we have taken swift and strong enforcement action in response to Russia's further invasion of Ukraine. But our work isn't stopping there. In the future, we anticipate making changes to our administrative enforcement policies, for both our export control and antiboycott laws, in order to increase transparency, strengthen compliance, and incentivize deterrence. These contemplated policy shifts, which I will touch on later, will be designed both to protect our country from these growing nation-state threats and to hold those that don't play by the rules accountable.

Before I get to future administrative enforcement changes, though, I want to provide some details on the Commerce Department's efforts to hold Russia accountable for its unjustified war against Ukraine. My Commerce colleague, Assistant Secretary Thea Kendler, and her team have worked in close coordination with an unprecedented coalition of U.S. allies and partners to impose far reaching export restrictions that limit Russia's ability to obtain the goods and technologies it needs to wage war.

This includes both expansive controls on dual-use items – items that can be used for both commercial and military purposes – in the fields of electronics, marine, and aerospace, including when certain items are produced abroad from U.S. software, technology, or equipment; controls on oil-field refinery equipment; controls on luxury goods like alcohol and cigarettes; embargoes on U.S. goods and technologies to specific Russian and Belarusian military groups that are helping Vladimir Putin; and last week's expansion of restrictions on Russian industrial and commercial sectors to align with European Union actions.

These stringent and sweeping export controls, along with similar controls on Belarus for enabling Russia's conduct, are designed to cut off Russia's access to the tools of war and undermine its strategic ambitions to exert influence on the world stage.

The controls are not just being imposed by the United States, but also by 37 allies and partners around the globe. It's the broadest expansion of multilateral export controls among like-minded partners since the creation of CoCom back in 1949. It's also a partnership for a similar purpose – to help counteract Russian aggression.

This powerful international response is already resulting in serious consequences for the Russian military and defense sectors. Our new export controls have helped degrade the Russian

military and defense base, including the production and operation of tanks, precision-guided missiles, military satellites, and intelligence and military systems dependent upon western electronics.

In the aerospace sector, companies have stopped selling spare parts or providing engineering and maintenance support to Russian airlines. Analysts predict that, in the near future, Aeroflot, Russia's premier commercial airline, will be unable to sustain even domestic flights without the parts necessary to maintain its aircraft.

And the story is the same across virtually every other Russian economic sector – from automobile to heavy machinery to advanced computing. Since February 24th, total U.S. exports to Russia have decreased nearly 80% in value compared with the same time period last year. We've witnessed companies not only comply with our rules, but some have gone further of their own accord. In effect, they have "self-sanctioned" to account for the reputational risk of staying in business with Russia. According to one study conducted by the Yale School of Management, as of Friday, 594 U.S. companies have suspended or scaled back operations in Russia and another 316 have exited Russia altogether.

When we work together with our allies, echoing the multilateralism of the CoCom days, export controls can achieve powerful results. Not surprisingly, we've found that companies are more likely to tolerate controls when they are held to the same rules as their competitors.

While it's good news that most companies have complied with the new controls, rest assured that we're taking vigorous action against those that don't. And that's where my team comes in on the enforcement side of the house. We have 130 federal agents stationed in 30 cities nationwide, who work in concert with more than 50 intelligence analysts, export compliance specialists, and Export Control Officers, to enforce the export laws.

Here's what we've done so far to enforce the new Russia rules.

First, we've put in screening mechanisms to identify all relevant exports to Russia. When someone files paperwork saying they're shipping something to Russia that's potentially covered by the new controls, we'll see it and then we can stop it. So far, since the first Russia rule went into effect on February 24, we've detained 166 shipments to Russia and Belarus and currently have over $77 million worth of exports under detention.

Second, we've put 260 parties with Russian defense affiliations on the Entity List, which means that they can't receive U.S. exports without a license and, under current policy, licenses will be denied. The companies added to the list include Russia's leading integrated circuit manufacturers, Russian space-based and satellite-based component manufacturers, Russian drone manufacturers, and Russian shipbuilding factories. Because of their entity listing, these companies can no longer get the U.S. parts they need to manufacture things for the Russian military.

Third, in the aerospace sector, we've publicly identified 157 airplanes that we believe were illegally exported to Russia and Belarus. By publicly identifying these airplanes, we are

putting the world on notice that if they service these aircraft, they are in violation of our laws and do so at their peril. I have also issued Temporary Denial Orders against four of Russia's biggest passenger and cargo airlines. These orders mean that the four airlines cannot receive U.S. parts for their planes. Over time, Aeroflot, Utair, Azur Air, and Aviastar 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.

Fourth, we know from data which U.S. companies had been exporting items to Russia that are now restricted. We're reaching out to these companies, both to educate them on the new controls and to make sure they're in compliance with the new rules. We've conducted 440 of those outreaches so far.

And fifth, we've opened a number of enforcement investigations. While our investigations take time to turn into public charges as we gather the necessary facts and evidence, my prediction is that, down the line, you'll see the results of that hard work – in the form of public charges against companies that are putting profits ahead of the welfare of the Ukrainian people.

So now that I've described the national security threat landscape, how our enforcement tools are central to combatting those threats, and the ways in which we've put those tools to use in support of Ukraine, I'd like to preview some future policy changes we're contemplating as part of an effort to further strengthen our enforcement posture. More specifically, we are going to be making some changes to our administrative enforcement programs in order to increase prevention, increase transparency, and incentivize compliance and deterrence.

Administrative sanctions, whether in combination with criminal penalties or alone, send a powerful message: implement effective compliance programs on the front end or risk penalties on the back end that will hurt both your reputation and your bottom line, either through stiff monetary penalties, or potential denial of export privileges, or both. Our view is that most U.S. companies are committed to doing the right thing and work hard to ensure that their sensitive technologies and goods don't end up in places where they could harm our national security. But, unfortunately, that's not uniformly the case. When faced with the stark choice of complying with the export laws or booking revenue, some companies choose mammon before country. Our view is that, in addition to our obligation to enforce the law when it's been violated, we also have an obligation to companies that are playing by the rules. If we are not vigorously enforcing against violators, then those companies that are obeying the law are unfairly disadvantaged in the marketplace.

With those considerations in mind, we're in the midst of a policy review focused on how we can best bolster our administrative enforcement. We want the world to know that criminal prosecution is an important tool in our toolbox and one we use aggressively when the facts warrant. But it's not our only tool. Our administrative penalties also have bite and, therefore, should have important deterrent effect. It's true that our administrative enforcement authorities do not result in individuals being sentenced to prison for their misconduct – only our criminal authorities permit that. But when it comes to companies, our administrative authorities can result in nearly the same punishment that a criminal conviction would bring – they permit us to impose

significant monetary penalties, to reach agreements requiring a corporate compliance overhaul, and, in extreme cases, to outright deny a company the ability to export. Other than the heavier reputational hit and the collateral consequences that can flow from a criminal conviction, our administrative enforcement authorities can be just as powerful as our criminal ones when it comes to cases against companies.

Given that powerful potential, we want to make sure we're doing everything necessary on the policy front to make our administrative authorities as nimble as possible. Here are a few specific areas we're reviewing where I anticipate possible changes in the future.

First, at present, our administrative charging letters are not public until after a case resolves. This means that the public doesn't know which companies we allege have violated our regulations until the matter is completed, often years later. Moreover, it means that companies that may be engaging in similar misconduct aren't fully disincentivized to stop, given that they aren't being shown a real time example of what happens when you break our rules. So, we're considering changing that policy to make charging letters public when filed, just like with the initiation of criminal charges or of administrative proceedings with the SEC.

Second, we're reconsidering our use of no admit/no deny settlements. In the past, when we have resolved administrative enforcement matters short of trial, we have allowed companies to pay a reduced penalty without admitting misconduct. While doing so makes it easier to reach such resolutions, no admit/no deny settlements also have two significant downsides. For one thing, it means there's no statement of facts that the company admits to – no factual recitation that lays out what the company did that got it into trouble. Without such an admitted statement of facts, it is more difficult for other companies to learn from their peers' mistakes and adjust their behavior accordingly. In addition, companies get a significant reduction in penalty when they resolve with us short of trial. That makes sense, as we want to incentivize companies to resolve matters. But in other enforcement contexts, companies must admit their conduct in order to qualify for the reduced penalty. Our concern is that without admitted facts, we may not be sending a deterrent message as strong as we believe warranted when the export laws are violated, especially given the magnitude of the national security threats those laws are designed to help combat.

Third, we're taking a look at penalty amounts. Again, I start from the premise that given how directly our export laws map onto today's national security threats, violations of those laws deserve commensurate punishment. Given the amount of federal resources it takes to gather the evidence necessary to bring one of these cases, and the national security stakes, penalties must be high enough to both punish and deter those who would violate the law. If penalties are low, it is too easy for companies to do a cost-benefit analysis and conclude that they would rather risk paying a small fine on the back end if they get caught than invest in compliance systems or forego revenue from sales they should be turning down up front.

In addition to the Office of Export Enforcement, I also oversee the Office of Antiboycott Compliance, which has administrative enforcement authority over our antiboycott laws. Those 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. Just as we are doing

with export controls, we are reviewing how our administrative penalties should apply to antiboycott violations. There too, we're evaluating whether no admit/no deny settlements make sense from an enforcement policy perspective and are weighing whether and how far to raise penalties for violations. As one step in this review process, I held a listening session last week with members of BIS's Regulations and Procedures Technical Advisory Committee, otherwise known as the RPTAC, to discuss a proposal to reprioritize the categories of antiboycott violations in a way that better aligns them with the violations' relative severity.

For both export and antiboycott enforcement, we are aiming to roll out policy changes in the coming months. Before we do, we are eager to hear from you if you have thoughts you would like to share.

Thank you to the Society for International Affairs for inviting me to deliver today's keynote address. It is an honor to be here and to have had the opportunity to share some thoughts with all of you. As I said at the top, the work we collectively do has never been more important and the national security stakes have never been higher. I am optimistic that our shared resolve and shared actions, combined with those of our domestic and foreign partners, will continue to help keep our country safe from harm. Thank you.

###