FOR IMMEDIATE RELEASE
June 21, 2023
www.bis.doc.gov

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

Assistant Secretary for Export Enforcement Matthew S. Axelrod Remarks to the American Association of Exporters and Importers' 102nd Annual Conference and Expo

As Prepared for Delivery

June 21, 2023

Thank you for the introduction. It's great to be here with all of you. Last week, I was in Phoenix for work. While there, I visited places called Biscuit Flats and Dead Man's Gulch. When I say those names, I'm sure it conjures up pictures in your head of dust, cactus, and tumbleweeds. Like something out of an old Western movie. And two years ago, that picture would have been accurate. The only thing missing would be the saloon with the swinging doors. But not anymore.

Today, rising from Biscuit Flats and Dead Man's Gulch is a building about as modern as modern gets. That's where Taiwan Semiconductor Manufacturing Company (TSMC) is constructing a state-of-the-art semiconductor manufacturing facility, known as a "fab." TSMC plans on producing advanced 5 nanometer chips there next year. Five nanometers. Do you know how small that actually is? A sheet of paper is about 100,000 nanometers thick. That means that five nanometers is 1/20,000th as thick as a sheet of paper. To put it another way, one nanometer is about as long as your fingernail grows in one second. So, look at your fingers and wait five seconds. The change in your fingernail length – that's how big we're talking.

The theme of today's conference is "Reshaping the Status Quo." When Biscuit Flats and Dead Man's Gulch are on the cusp of churning out microchips that are 1/20,000th as thick as a sheet of paper, or equivalent to five seconds of fingernail growth – I think it's fair to say the status quo is being reshaped.

* * *

And that reshaping of the status quo when it comes to the scale and power of our technological advances is paralleled by a reshaped status quo when it comes to our national security. We're at an inflection point there, too.

In 2006, the Office of the Director of National Intelligence (ODNI) published the Intelligence Community's first Annual Threat Assessment, which catalogues our country's most pressing national security threats. The 2006 report began with a discussion of the threat of terrorism, from non-state actors like al-Qaeda. Analysis of the threat posed by Russia did not appear until page 16 and the discussion of China wasn't until page 20. As you can imagine, this year's report is very different. For 2023, the Annual Threat Assessment leads with nation-state actors: China, Russia, Iran, and North Korea. Part of why these nation-state actors now come first in the report is because they are trying to use advances in technology to surpass us militarily. They seek to acquire sensitive U.S. technology to advance their military capabilities – with their ultimate goal being to shift the world's balance of power.

It is critical we ensure that these advanced technologies work for, not against, democracy and security. Technologies like hypersonics, quantum computing, and artificial intelligence, for example, have the potential to refine and reshape the geopolitical landscape. The experts assess that, eventually, quantum computing will enable the country that sufficiently develops the technology first to create unbreakable encryption, and to break all existing encryption, revealing sensitive national security communications and exposing sensitive economic data. Imagine if the first country to get there first is one of the four listed in this year's Annual Threat Assessment.

Our tools are now a spot-on match for confronting this most pressing national security challenge. Our mission is singular: keeping our country's most sensitive items out of the world's most dangerous hands. It is critical that we prevent sensitive U.S. technology from ending up where it shouldn't overseas.

As Assistant Secretary for Export Enforcement, I lead a team of law enforcement agents across the country, paired with analysts at headquarters, dedicated to this mission. Our enforcement authorities are broad, allowing us to bring both criminal charges (with our colleagues at the Department of Justice) and administrative enforcement actions through in-house lawyers at Commerce. We also nominate parties to the Entity List when they are involved in activities contrary to the national security or foreign policy interests of the United States. And while a a number of U.S. government agencies can nominate parties to the Entity List, the vast majority of nominations come from our enforcement analysts.

* * *

Given these mind-boggling advances in technology and the change in the national security threat picture, we're intently focused on making sure our tools are maximally effective. This has led to enforcement policy shifts over the past year, in addition to new enforcement partnerships. Let me spend a few minutes talking about each. On the policy front, we've made a number of changes to help strengthen our administrative enforcement program. I'll highlight just a few of the changes here.

First, we changed our regulations, so our charging letters are now public when filed rather than only down the road when there's a resolution. This change allows the exporting community to know in closer to real time what type of conduct gets you in trouble. It also provides an incentive for companies to resolve matters with us sooner rather than later.

Second, we got rid of "no admit, no deny" settlements. It used to be you could resolve with us and pay a penalty, but never admit you actually did the conduct we alleged. No longer. Now, our resolutions require you to admit that you did the conduct. That's why, a few months ago, when we entered into a $300 million resolution with Seagate Technologies – the largest standalone penalty ever imposed by BIS – the company admitted that it continued to sell hard disk drives to Huawei after we imposed the Huawei foreign direct product rule, and after its only two competitors had stopped selling.

Third, we recently clarified our regulations concerning voluntary self-disclosures and disclosures about the conduct of others. The work we do is a shared endeavor with industry. We don't want your technology going where it shouldn't and neither do you. We rely on you to come tell us when something went wrong. We want to hear from you whether you discovered a potential violation of our rules by your own company or by someone else. Either way, we want to hear it. That's why, for voluntary self-disclosures, we sharpened the risk calculus. People have long understood that if you find out about a significant potential violation, and you report it to us, you get concrete credit in the form of a sharply reduced penalty. Now, if you uncover a significant potential violation but affirmatively choose not to report it, and we later find out, we will consider that an aggravating factor in your penalty calculation. In other words, , it's better to knock on our door before we knock on yours.

On disclosures about the conduct of others, we want to incentivize companies to tell us when other companies are violating our rules. The goal is a level playing field. The last thing we want is for a company to feel like a chump for following our rules because they're watching their competitor ignore the rules and continue to make sales. But we can't act on things we don't know about. So, we made clear that, under our regulations, if you provide a tip about another company that leads to an enforcement action, we'll remember it and take it into consideration if you ever get in trouble with us down the line. That is, we will consider your tip "exceptional cooperation," and will count it as a mitigating factor if a future enforcement action, even for unrelated conduct, is ever brought against you.

* * *

So those are some of our enforcement policy initiatives. Let me turn to some of our partnerships.

I outlined the seriousness of the threat earlier. One primary way we're combatting that threat is through the newly established Disruptive Technology Strike Force, which I co-lead with Assistant Attorney General for National Security Matt Olsen at the Department of Justice. The Strike Force has 14 local cells across the country, which each include a federal prosecutor plus agents from Commerce, Homeland Security, and the Federal Bureau of Investigation. These local cells are supported by an interagency analytic cell here in Washington, D.C.

The purpose of the Strike Force is to focus and prioritize enforcement efforts to prevent our adversaries from advancing their development of these disruptive technologies – like quantum, like hypersonics, like artificial intelligence. The Strike Force uses an all-tools approach, including everything from criminal indictments to administrative actions to industry outreach. And it's not just the most heavily controlled pieces of technology – many disruptive technologies rely on uncontrolled items. If there's a particular widget that allows the quantum computer to run, we care about that too.

The Strike Force is already delivering results. A month ago, we announced the first five cases brought in U.S. Attorney's Offices across the country, from New York to California. The cases involved everything from alleged procurement networks created to help the Russian military and intelligence services obtain sensitive U.S. technology, to defendants allegedly stealing source code from U.S. technology companies to market it to Chinese competitors. One case, out of the Southern District of New York, alleges that a Chinese procurement network worked to provide Iran with materials used in weapons of mass destruction and ballistic missiles. In addition to arrests and indictments, we also announced a related temporary denial order suspending the export privileges of several defendants, a Russian airline, and a freight forwarder for sending U.S. aviation parts and electronics to Russia. Although the cases are all different, there's a throughline – we're focused on keeping countries of concern from getting the technology they need to help advance their militaries.

The Strike Force is supported by other interagency partnerships we've developed. We've partnered with Treasury to put out the first two ever joint alerts between FinCEN and another agency. The alerts provide financial institutions and exporters with guidance on how to spot indicators of evasion of our Russia controls. And they give banks a specific code to use when filing Suspicious Activity Reports (SARs). A code that our analysts can then search the SAR database for and use to send leads out to the Strike Force cells or compose Entity List nominations.

We also, along with the Department of Justice (DOJ) and the Department of the Treasury, issued a tri-seal compliance note for industry focused on Russian evasion tactics. And just a few weeks ago, we did a quad-seal advisory along with DOJ, Treasury, and the State Department to highlight both the threat of Iran's drone program and the need for industry to take appropriate steps to prevent activities that would support its further development.

We are also partnering with academic research institutions through our Academic Outreach Initiative. We're working with specific universities to help them protect their sensitive research from nation-state actors who seek to exploit our open, collaborative academic environment.

And we're collaborating with foreign coalition counterparts, like our Five Eyes partners, to coordinate on enforcement issues. We are also coordinating with our European partners, both bilaterally and through the U.S.-EU Trade and Technology Council. And we're partnering with ASEAN countries like Singapore, Malaysia, and the Philippines as well.

We've long had an international presence to help prevent diversion, through our Export Control Officer, or ECO, program. We recently added two new ECO positions, one in Helsinki and the other in Taipei. We have also, for the first time ever, embedded an enforcement analyst abroad. We've sent one of our analysts to Ottawa to liaise on export controls directly with the Canada Border Services Agency and our other Canadian partners.

Finally, we're traveling to spread the word. I recently went to Kazakhstan and Kyrgyzstan with colleagues from the Department of the Treasury and the sanctions coordinators from the United Kingdom and the European Union to talk to those governments about countering the evasion of our Russia controls. While there, we met with government officials and the private sector to share information, outline strategic priorities, and offer assistance to help facilitate compliance.

* * *

Let me turn now to a partnership that, while not a new one for us, is an absolutely critical one: our partnership with industry. At the Bureau of Industry and Security, we regularly interact with industry – in fact, we consider it a cornerstone of what we do. As I mentioned earlier, export controls are a shared endeavor, and industry is the primary line of defense. No one knows your business, and the export control risks inherent in it, like you do. As I've said repeatedly, we'd much rather help those of you in industry comply on the front end than have to enforce on the back end. When we enforce, it often means the item has already ended up where it shouldn't, and the national security harm has already happened.

If you don't know your local Office of Export Enforcement agent, please reach out and get to know them. We have agents in 30 locations across the country. We have 12 dedicated offices and another 18 locations where our agents are co-located with another federal law enforcement agency. But no matter where you are, even if not in one of those 30 locations, there's an agent responsible for your geographic area.

While our partnership with industry isn't new, what is new is the increased importance of export controls and export enforcement. You need to understand that not paying attention to export controls now presents enterprise risk. Our regulations and our policies are being updated frequently, at a pace higher than in the past. And they're more expansive than in the past as well.

At the same time, as I mentioned earlier, we are enhancing our enforcement posture. Enforcement of our export controls is a top priority not just for us but also for our partners at the Department of Justice. That means that when companies do not invest in compliance up front, they're going to pay the price on the back end – with large fines and reputational consequences.

As they used to say in the old days of Biscuit Flats and Dead Man's Gulch, there's a new sheriff in town. You don't want to get this wrong. And we don't want you to get it wrong. So reach out to us for help. We're ready and willing partners.

Thank you.

###