FOR IMMEDIATE RELEASE
July 26, 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 to the Society for International Affairs Summer Back to Basics Conference

July 26, 2023

Last month, I noticed a few streets closed outside my office at the Department of Commerce. That's not unusual, given our close proximity to the White House. But these street closures were different. In addition to the typical barricades, the streets were filled with giant camera booms, dollies, cranes, and what seemed like miles of extension cords. Turns out, they were filming a Captain America movie, which will add to the roster of more than 30 superhero films that comprise the Marvel Cinematic Universe.

What's interesting about the fictional universe Marvel has created is that it's a shared one. In other words, the superheroes who inhabit it do so in an extended web of interconnected plots, crossovers, sequels, prequels, and spin-offs. There are stand-alone movies, where one character, like Iron Man, is showcased. And there are movies like the Avengers, where an ensemble cast of Marvel's most powerful superheroes team up to vanquish a collective evil. The Marvel universe is not only a shared one, it's also a ridiculously popular one. Out of the top fifteen highest grossing movies of all time, six are Marvel movies.

Now, you may be asking why I'm bringing up comic books at an export control conference. It's because we too inhabit a shared universe. Export controls are inherently interconnected. When a country acts unilaterally, its actions can be self-defeating – the country burdens its own companies while the bad guys still get the technologies they need from other countries to modernize their military or advance their weapons-of-mass-destruction program. As one former Bureau of Industry and Security ("BIS") Under Secretary used to say, imposing unilateral controls is like damming half a river. That's why so much of the export control universe involves multilateral or plurilateral controls.

Likewise, on the enforcement side, our universe is a shared one too. As I'll discuss in some detail today, our efforts are ever more intertwined with those of our U.S. government partners,

including through our Disruptive Technology Strike Force and our work with Treasury Department components. They're also increasingly connected with the efforts of our foreign enforcement counterparts, including Five Eyes and G7 countries. And perhaps most importantly of all, our efforts are linked with those of industry and academia – our primary line of defense against foreign adversaries. The people on the frontlines, whether in a company or a university, are the ones best positioned to notice when a customer's or research partner's request seems off, or when something anomalous appears. When their Spidey-sense tingles, there's a reason. Simply put, when it comes to ensuring compliance with our export laws, it's not just my team doing the work. It's the entire export enforcement universe – one that's filled with real-life superheroes.

* * *

Given that this is SIA's Summer Back to Basics Conference, I want to provide you an overview of the Export Enforcement side of BIS – what we do, why it's important, and what we've been working on.

What we do. As Assistant Secretary for Export Enforcement, I lead a team of law enforcement agents and analysts dedicated to preventing sensitive U.S. technology from ending up where it shouldn't. Our enforcement authorities are broad, allowing us to bring both criminal charges (with our colleagues at the Department of Justice) and administrative enforcement actions (with our Commerce Department lawyers). We also nominate parties to the Entity List if they are involved in activities contrary to the national security or foreign policy interests of the United States. While various U.S. government agencies can nominate parties to the Entity List, the vast majority of those nominations come from our enforcement analysts.

Why it's important. In 2006, the Office of the Director of National Intelligence ("ODNI") published the Intelligence Community's very 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 quite 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, at the same time, it will allow that country to break all existing encryption, revealing the world's most sensitive national security

communications. Imagine if the 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. But just because we have a singular mission doesn't mean we do this work alone. To the contrary, the magnitude of the challenge we face requires joint efforts and partnerships.

Which brings me to what we've been working on – with our U.S. government partners, with our international partners, and with our industry partners.

* * *

I'll start with our recent efforts to strengthen our partnerships within the U.S. government. Earlier this year, we and the Department of Justice ("DOJ") established the Disruptive Technology Strike Force, which I co-lead with Matt Olsen, the Assistant Attorney General for National Security. The mission of the Strike Force is to target illicit actors, protect supply chains, and prevent critical technology from being acquired by authoritarian regimes and hostile nation-states.

To achieve this mission, we've established 14 local cells around the country, each of which includes a federal prosecutor, an agent from BIS, a Homeland Security Investigations agent, and an agent from the Federal Bureau of Investigation. Each of the 14 cells work together to investigate and prosecute violations of U.S. export laws. The cells are also supported by an interagency analytic cell in Washington, D.C.

The Strike Force is already delivering results. In May, we announced our first five cases, which originated in U.S. Attorney's offices around 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.

We've also strengthened our partnership with the Treasury Department, particularly with the Financial Crimes Enforcement Network ("FinCEN") and Office of Foreign Assets Control ("OFAC"). Alongside FinCEN, we've published two unprecedented joint BIS-FinCEN alerts designed to educate financial institutions about export control evasion and how to spot it. The joint alerts highlight specific items that Russia needs for its military, including its missiles and unmanned aerial vehicles, as well as ways to identify and report evasion red flags. They contain a unique key term for financial institutions to use when filing Suspicious Activity Reports (SARs) related to evasion of the Russia controls. That key term has now been included in over 300 SARs – nearly one third of which have helped predicate new investigations, advance existing investigations, or develop Entity List packages. We are currently working with FinCEN

to find additional ways to notify financial institutions of export control evasion trends more broadly beyond our Russia controls and to support financial institutions' reporting of activities that contribute to those trends.

I'm announcing today that we just signed an agreement with OFAC formalizing our close coordination and partnership. My team and I already meet regularly with our counterparts at OFAC. Now, we'll ensure that our enforcement teams are working even more closely together. Among other things, we'll be seeking to jointly resolve investigations of common subjects, including matters voluntarily disclosed to both agencies. As a result, you can expect to see more coordinated enforcement actions from us going forward.

* * *

To be clear, our government isn't the only one with whom we've strengthened partnerships. We've also been working hard to broaden our partnerships with foreign governments. On Russia specifically, our colleagues on the Export Administration side of BIS built a coalition with 38 other governments to put in place the most comprehensive export controls in history aimed at a specific country. Together with our partners, we've limited Russia's access to specific technologies and other items needed to sustain its illegal military activity in Ukraine. Multilateral controls, especially when part of a coordinated international endeavor to apply economic pressure on a specific country, are incredibly powerful.

On the enforcement side, we're working closely with foreign counterparts across the world to enforce these controls. Late last month, I was in Ottawa meeting with our Five Eyes partners from Canada, the United Kingdom, Australia, and New Zealand, where we announced a commitment to formally coordinate on export control enforcement. We agreed that we will increase collaboration and information sharing across our respective enforcement teams. We'll share export enforcement best practices and enhance our abilities to prevent malign actors from evading our respective controls. By leveraging each other's strengths, we will enhance our collective security. We have also – for the first time ever – stationed an enforcement analyst abroad. We now have an enforcement analyst in Ottawa to liaise on export controls directly and daily with the Canada Border Services Agency and our other Canadian partners.

In addition to our work with our Five Eyes allies, we are also partnering with the other G7 members (Canada, the United Kingdom, France, Germany, Italy, Japan, and the European Commission) to close evasion pathways and disrupt Russia's ability to source inputs for its illegal war. This past April, our Deputy Secretary, Don Graves, along with his counterparts from the Treasury Department and the Japanese Finance Ministry, convened a meeting of the G7 countries to announce a new enforcement coordination mechanism. This effort is designed to bolster coordinated international enforcement of the multilateral sanctions and export controls on Russia. There is widespread agreement that it's not sufficient for allied countries to have established complementary controls on paper. We also need to work together to enforce those controls in a complementary way. Earlier this month, we held the first working-level meeting of

this G7 enforcement coordination mechanism, where we committed to leverage our collective enforcement capabilities. Just like our Five Eyes effort, by working closely with our international enforcement counterparts, we are strengthening security for everyone.

* * *

Let me turn now to our partnership with industry. As I mentioned earlier, export controls are a shared universe, and no inhabitant of that universe is more important than industry. Put simply, industry is our first line of defense. No one knows a company's business, and the export control risks inherent in it, like the company itself does. As I've said repeatedly – and as recently as last week in a post on the Compliance and Enforcement Blog hosted by New York University School of Law's Program on Corporate Compliance and Enforcement – we would much rather work with companies to prevent violations on the front end than enforce violations on the back end. When we enforce, it often means the technology has already gone to our adversaries and the national security harm has already occurred. Our goal, which I know is a shared one, is to avoid getting to that point whenever possible.

Our work enforcing the Russia controls provides a concrete example. Beyond our enforcement efforts, U.S. and international industry have been essential players in preventing Russia's access to key technologies. Our agents have reached out to more than 800 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. I've also been contacting specific companies and trade associations involved in the manufacture or distribution of components that Russia needs for its missile and drone programs in order to share diversion prevention strategies.

We've also put out written Russia-related guidance to industry. In March, we issued a first-ever tri-seal compliance note for industry with DOJ and the Department of the Treasury, focused on Russian evasion tactics. And in June, we did a first-ever quad-seal advisory along with DOJ, Treasury, and the Department of State to highlight 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. That's all in addition to the joint BIS-FinCEN alerts on Russia I mentioned previously.

And our guidance is not limited to Russia or to evasion tactics. Just today, for example, we issued a second tri-seal compliance note with DOJ and Treasury, highlighting our respective voluntary self-disclosure policies. As discussed in the note, we recently clarified our regulations concerning both voluntary self-disclosures and disclosures about the conduct of others. The new compliance note discusses these clarifications, along with recent changes to the National Security Division's VSD policy and FinCEN's whistleblower program.

In addition to industry, we also partner closely with academia. Last June, I announced our Academic Outreach Initiative. Given the increasing interconnections between the domains of

national security and academia, we are partnering with prioritized universities to help them protect their research from foreign government adversaries. Last year, we established partnerships with 20 universities whose work gives them an elevated risk profile. In addition to providing each of these universities with a dedicated "Outreach Agent" to serve as their point of contact, we conducted webinars and trainings on topics such as red flags specific to academia and how to best conduct open-source research and due diligence on academic partners. Today, I can announce that we've expanded this effort. I recently invited nine new universities to the Initiative. They'll join the existing twenty in receiving a dedicated agent, training, and briefings as part of this important effort to protect the sensitive technologies that can result from advanced academic research.

* * *

Our partnership with industry goes beyond partnership on export controls. I also oversee the Office of Antiboycott Compliance, which enforces the antiboycott rules and works closely with companies to support their compliance with those rules. The antiboycott laws, implemented under the Export Administration Regulations, prohibit U.S. companies from taking certain actions in support of an unsanctioned foreign boycott of a country friendly to the United States, such as the Arab League boycott of Israel. The provisions also prohibit U.S. persons from complying with certain requests for information designed to verify compliance with such a boycott.

Last October, we strengthened our antiboycott enforcement program by making changes designed to enhance compliance, increase transparency, incentivize deterrence, and compel accountability. We instituted a requirement that companies entering into settlement agreements for antiboycott violations admit to a statement of the facts outlining their conduct. We raised our penalties. And we announced a renewed focus on foreign subsidiaries of U.S. companies and said we would explore additional ways to deter foreign parties from issuing or making boycott requests. Our efforts have borne fruit. In May, for example, we imposed a civil penalty of $283,500 against Regal Beloit FZE, a foreign subsidiary of a U.S. company located in the United Arab Emirates, to resolve alleged violations of the antiboycott regulations. The company failed to report to us that it had received 84 requests during a period of more than four years from a Saudi Arabian customer to refrain from importing Israeli-origin goods into Saudi Arabia. The company voluntarily self-disclosed the violations, cooperated with the investigation, and took remedial measures after discovering the conduct at issue – otherwise the penalty would have been even higher.

Today, I'm announcing further actions to strengthen antiboycott reporting and compliance. As detailed in a memorandum that I distributed to our workforce this morning, we are implementing two new measures:

First, we have modified the boycott reporting form. Prior to today, U.S. persons were required to report to us when they received a boycott-related request and required to identify the country

from which the request originated. But they weren't required to tell us the identity of the specific party who made the request. Starting today, our reporting form will also require the identification of the requesting party. This information will help us investigate and hold accountable any foreign subsidiaries or affiliates of U.S. companies that make unlawful boycott-related requests.

Second, we have placed an antiboycott policy statement on U.S. acquisition management websites. Yesterday, we posted a policy statement on both the Department of Commerce's Office of Acquisition Management website and the broader federal contractor SAM.gov website. The policy statement clearly articulates the requirements of the antiboycott regulations and their applicability to U.S. government acquisition contracts. By adding the policy statement to these websites, we're notifying federal contractors that they must abide by the antiboycott regulations as part of their contractual responsibilities, especially if they want to do business with one of the world's largest procurement organizations.

Compliance with the antiboycott regulations is not optional. All U.S. companies – whether federal contractors or not – should familiarize themselves with the antiboycott regulations and reporting requirements. And if you have any questions, please visit our website or call the Office of Antiboycott Compliance advice line. Our team stands ready to partner with you on antiboycott compliance.

* * *

A little over a month ago, there was a long New Yorker article on the Marvel Cinematic Universe and how it came to exist. Reading the article, I was struck by one particular line, which said that "[m]ost plots boil down to 'Keep glowy thing away from bad guy,' and the stakes are nothing less than the fate of the world, which come to feel like no stakes at all." I think the article meant this as a criticism of Marvel movies' repetitive storylines, implying that audiences might get bored because when, for each movie, "the stakes are nothing less than the fate of the world," then over time they can "come to feel like no stakes at all."

I want to assure you that, for both my team and for everyone who does export enforcement, who focus day in and day out on keeping our country's most sensitive items out of the world's most dangerous hands – or, in other words, "keep[ing] glowy thing away from bad guy" – the work is never boring. We know the stakes. Those stakes are incredibly high. And they never come to feel like no stakes at all. Thank you.