FOR IMMEDIATE RELEASE
January 16, 2024
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 NYU School of Law's Program on Corporate Compliance and Enforcement

January 16, 2024

Thank you, Joe, for that introduction and to the NYU School of Law's Program on Corporate Compliance and Enforcement for hosting me.

I spent some time over the holidays with family, as I hope everyone here did. We visited my wife's parents in Florida, where my father-in-law played us a few records on the 1947 Rock-Ola jukebox he lovingly restored. His Rock-Ola jukebox is brightly colored, with swirling lights and intricate grill work. But it's also the size of a cabinet, difficult to move anywhere, and plays a grand total of 20 songs. That was state of the art in 1947.

Meanwhile, my daughters spent time during our vacation listening to their music on Spotify. From handheld mobile phones, they are able to access Spotify's library of over 100 million songs. During my father-in-law's lifetime, we've gone from 20 songs to over 100 million, from a large heavy object to an app that exists in the ether, accessible from anywhere. That pace of technological development, of commercial ingenuity, is breathtaking.

Rock-Ola itself is an exemplar of commercial ingenuity, but in a way you might not expect. In the early 1940s, during World War II, the country didn't need jukeboxes – it needed rifles. Rock-Ola answered the call and transformed its jukebox plant in Chicago to one that manufactured M1 carbines for the U.S. military. The M1 carbine replaced the earlier (and heavier) M1 rifle, which was difficult for soldiers to carry and impacted their range of motion. According to Rock-Ola's website, until 1944, they were "one of only 11 contractors for these operations, delivering completed military rifles at a rate exceeding 10,000 per month." The work it took to pull this off was extraordinary. The company had to "completely retool, recruit many hundreds of new employees, train them up and engineer numerous complex precision parts." They even took an old bunker underneath their factory parking lot and converted it into a shooting range. When the war ended, Rock-Ola stopped making rifles and ramped up their

production of jukeboxes. Their first post-war jukebox came off the line in 1946. My father-in-law's was manufactured just one year later.

* * *

Just as music technology has leapt forward from jukeboxes to streaming services, military technology has come a long way from the days of the M1 carbine. Instead of being limited to that rifle's maximum effective range of 300 yards, weaponized drones can fly for hours, if not days, traveling thousands of miles. And hypersonic missiles are even more advanced, traveling in excess of Mach 5, or over five times the speed of sound. Disruptive technologies like supercomputers, artificial intelligence, and hypersonics may eventually be powerful enough to deliver overmatch to whichever country first fully develops their military capacity, with the potential to alter the balance of power in the world.

As stated in President Biden's most recent National Security Strategy, "technology is central to today's geopolitical competition and to the future of our national security, economy and democracy." In other words, a critical part of our overall national resilience now rests both on our ability to innovate new technologies and on our ability to protect these technologies from being used – or misused – by our adversaries. That "protect" part is where my team comes in.

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.

It's American companies and universities that are at the forefront of innovating advanced technologies – like the 3D modeling software developed by students in NYU's Institute for Invention, Innovation, and Entrepreneurship – that will increase the security and prosperity of the American people. It's our job in Export Enforcement to help protect those technologies from adversaries who seek to obtain and misuse them to modernize their militaries, commit human rights abuses, or advance their weapons of mass destruction programs.

Our mission has changed significantly over the past decade. As these technologies have grown exponentially more powerful, the importance of the role that export controls play in protecting them, and by extension our national security, has grown in parallel. Export controls and their enforcement are at the forefront of our national security efforts like never before. As I said in a post last year on PCCE's Compliance and Enforcement blog, we're in a new era of export enforcement.

But there's a wrinkle. Our budget – aptly described by Commerce Secretary Gina Raimondo as still less than "the cost of a few fighter jets" – has not kept pace with the heightened importance of our mission. I have approximately 150 enforcement agents to cover the entire country. By comparison, the Department of Homeland Security's HSI has more agents than that in Tampa,

Florida alone. One direct consequence of this funding lag is that we are constantly aware of the need to strategically prioritize our finite resources so that we can best maximize our national security impact. We are continuously looking for ways to ensure that we're spending our time on the most consequential work. And we're continuously looking for partners to do it alongside us, thereby expanding our work's reach and impact.

That's what led us to establish the Disruptive Technology Strike Force, which I co-lead with Matt Olsen, the Assistant Attorney General for National Security at the Department of Justice (DOJ). The Strike Force works to protect a prioritized group of advanced technologies from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran. To do that, we've brought together experienced agents and prosecutors in fourteen locations across the country, including here in Manhattan and across the river in Brooklyn. These agents and prosecutors are supported by an interagency analytical effort in Washington, D.C. By partnering closely with other enforcement agencies, and by focusing our combined efforts on the technologies we're most concerned about, we're putting our finite resources to their highest and best use.

This strategic effort to deploy our resources for maximum national security impact similarly led us to work with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) to develop the first-ever "key terms" for banks to use when filing Suspicious Activity Reports (SARs) related to export control evasion. Prior to our work with FinCEN, banks had no uniform way to code SARs related to export control evasion. This meant that our analysts had to hunt through haystacks of SARs looking for the needles of SARs that were filed because the bank suspected a potential export violation. Now, our analysts are able to simply review the SARs that contain either of the two new key terms – one for Russia evasion and one for evasion in the rest of the world. Our partnership with FinCEN has allowed us to maximize our analysts' time by focusing their efforts on evaluating the SARs most likely to yield actionable leads. To date, we have reviewed over 500 of these SARs, and we have been able to action nearly twenty percent of those filings in various ways, including by cutting leads to our enforcement agents, advancing existing cases, and developing Entity List packages.

In addition to working with partners to prioritize our efforts and maximize our impact, we've also made internal adjustments. This past October, at the start of our fiscal year, we changed the categories of what we measure internally, to help us better drive our prioritized enforcement efforts. More specifically, we launched a new metrics initiative – how we track our investigative and analytic work – so that we can best evaluate how close the fit is between our highest priorities and how we are spending most of our time. Now, for the first time ever, the annual performance plans for all of our managers include a component on how well their field office's investigations, or leads generated by their analysts, connect to our highest-priority areas. More specifically, we are focusing on the items of most concern – like the disruptive technologies I mentioned earlier; the end users of greatest concern – like adversarial military, intelligence, and security agencies as well as transnational criminal organizations; and the end uses of greatest concern – like WMD, destabilizing military modernization efforts, and human rights abuses.

With this enhanced focus, we can better ensure that our agents and analysts are spending their time where it can have the maximum impact.

* * *

It's not just the Strike Force, the new key terms with FinCEN, and our metrics initiative. We made changes to our voluntary self-disclosure (VSD) program with the same goal in mind: to help prioritize our resources to best meet the most pressing national security threats.

First, in 2022, we amended how we process VSDs. For those VSDs involving minor or technical infractions, we now 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 do a deeper dive to determine whether administrative or criminal enforcement action may be warranted, while at the same time ensuring that companies get significant credit when they come forward voluntarily. By fast-tracking the minor violations while assigning agent and attorney resources to the more serious ones, we are using our finite resources more effectively while also allowing companies that submit minor or technical VSDs to receive a quicker response.

And last April, we clarified our VSD policies with the goal of driving additional disclosures of significant possible violations of the EAR. When a company thinks about whether or not to disclose an apparent violation, we want them to consider two additional factors: first, that a deliberate non-disclosure of a significant possible violation of the EAR is now considered an aggravating factor under our penalty guidelines. And, second, that if you don't tell us yourself, your competitor might -- because we now give them cooperation credit for doing so.

Let me take each in turn.

When someone chooses to file a VSD, they get concrete benefits; when someone affirmatively chooses not to file a VSD, we want them to know that they risk incurring concrete costs. In other words, when a company's export compliance program uncovers a significant possible violation, we want company leadership to consider not only the risks of disclosing, but the risks of not disclosing. And one of those risks is that we now consider the decision not to disclose as an aggravating factor under our guidelines.

Further, companies cannot sidestep the "should we or shouldn't we disclose" decision by self-blinding and choosing not to do an internal investigation in the first place. The existence, nature, and adequacy of a company's compliance program, including its success at self-identifying and rectifying compliance gaps, is itself considered a "general factor" under our settlement guidelines. This means, for example, that the presence or absence of an effective internal compliance program that uncovers export violations can either mitigate or aggravate a penalty.

For disclosures concerning the misconduct of others, we want to do everything in our power to encourage a level playing field. But it's impossible for us to punish violations we don't know about. We don't want a company that's complying with our rules and forgoing sales to suffer in silence while their competitors continue to book revenue. We want them to reach out to us. We will aggressively investigate and, when appropriate, take action. And if we do take action, there's something in it for the company that tipped us off. If the tip results in enforcement action, we'll consider it "exceptional cooperation," which is a mitigating factor under our settlement guidelines. In other words, the company that tipped us off gets credit in the bank with us if a future enforcement action, even for unrelated conduct, is ever brought against them.

* * *

Before I announce some further enhancements to our VSD program today, I want to give you a status report on the prior changes I just described. I'm often asked if these changes are working. The answer is yes – in at least three different ways. First, we're receiving more VSDs of potentially serious violations than ever before. Second, we're getting the minor or technical self-disclosures resolved more quickly than ever before. And third, we're seeing more disclosures about misconduct by others than ever before.

This past fiscal year, we saw an increase in VSDs that we marked as our highest priority – in other words, self-disclosures of potentially serious violations rose. Specifically, we received nearly 80% more VSDs containing potentially serious violations in FY2023 than we did in FY2022. This increase in the more significant VSDs occurred even as the number of overall VSDs remained relatively constant – at nearly 500 – from FY2022 to FY2023.

Second, we are resolving the minor or technical self-disclosures faster than ever before, which lets our agents focus more of their time on the more serious violations. The average processing time for a minor or technical disclosure is well under the 60-day window provided by the policy. As a result of our fast-track system, agents are able to resolve the smaller matters more quickly and focus their efforts on the most pressing cases. This is a win for everyone – for minor or technical disclosures, companies get a faster response, while we can conserve our resources for the most serious violations.

Finally, we're receiving more disclosures about misconduct by others than ever before. Since last April's policy announcement, we have received 33% more tips from industry than we did in the same time period – from April to December – the prior year. And that's in addition to the tips we've received this past year from the FinCEN whistleblower office, following FinCEN's expansion of their whistleblower program to include violations of the International Emergency Economic Powers Act (IEEPA) and "related actions" including violations of the Export Control Reform Act (ECRA).

The bottom line here is that our policies are working. The disclosure pattern over the past year – with the increases in serious disclosures and in tips about misconduct by others – has allowed us

to focus our investigative resources on the matters most important to protecting our national security.

* * *

All of that said, there is still more we can do to further this prioritization effort. That's why, this evening, I'm publicly announcing four new enhancements to our VSD program. I told our workforce about these enhancements earlier today, through a policy memorandum that we're also making public on our website. And we're also launching a newly revamped VSD webpage, which contains further specifics on the policy updates and is designed to help facilitate the submission of disclosures.

We recognize that it's not just my team at Export Enforcement that has finite resources. All of us – government, industry, and academia – live in a world of tight budgets. We want to ensure that our policies are designed to drive the prioritization not just of our resources, but of yours too. In other words, we want you spending most of your compliance dollars on preventing (and, if unsuccessful in preventing, then disclosing) the most serious export violations. To help drive this behavior, we're making some changes to reduce the administrative burden associated with submitting disclosures for more minor or technical violations, *i.e.*, those without aggravating factors.

First, for minor or technical violations there is no longer any need to disclose them individually. Instead, we are asking that such violations be bundled together to form a single overarching submission sent to us on a quarterly basis. Our aim is to further streamline the process for these smaller infractions, which should help conserve company compliance resources for the more serious violations. At the same time, it will allow us to conserve enforcement resources and more easily fast-track responses.

Second, companies can now submit an abbreviated "narrative account" for minor or technical infractions. Prior to today's updates, most companies were conducting and submitting a full review of apparent export violations over the prior five years as part of every self-disclosure. And they were submitting significant documentation to us as well. Now, we've made clear that, when it comes to minor or technical violations, we instead want companies to submit a succinct narrative account that focuses only on the most immediate violation. This shorter narrative does not need to include a five-year lookback or the accompanying documentation outlined in our regulations, unless we request it in an individual case. Our updated VSD webpage outlines the specific content required for this new abbreviated narrative account. By simplifying the disclosure process for minor or technical violations, we're encouraging companies to prioritize the more serious violations, where we continue to recommend a thorough review for the preceding five years.

Third, seeing as how it's now 2024, we figured it was about time to enter the 21st century and urge everyone to submit their VSDs by email. Electronic submissions will allow us to more

effectively receive, monitor, and track disclosures. The email address for submissions can be found on our updated VSD webpage.

Fourth and finally, we've clarified – and simplified – the process for how we handle requests to take corrective action for unlawfully exported items. Parties who become aware that an item has been unlawfully exported often seek to take corrective action to get that item back into the lawful stream of commerce. That's something we want to encourage. But the way our regulations work, once a party has knowledge that a violation has occurred in connection with the item, they are prohibited from taking further actions, such as transferring, storing, or disposing of the item. In such situations, parties need to request special permission to engage in these otherwise prohibited activities. Today, we've made some changes to help expedite these requests. For those interested in the specifics, the details are available in the policy memorandum and on our updated VSD webpage.

Collectively, these changes should help further drive prioritization. The prioritization of your time – and ours – so that it's spent on the most significant threats to our national security.

Just like with our metrics initiative, the new SAR key terms, and the Strike Force, we're taking action to ensure we're using our finite resources in the most impactful way. We're focusing our efforts on those export violations that cause the most harm to U.S. national security. We want companies and universities to follow suit. We want you to implement export compliance programs that identify and disclose potentially significant violations, not just minor or technical ones. We want you to tell us when others have committed potentially significant violations so that we can take action and ensure a level playing field. And we want to get illegally exported items back into the legal stream of commerce as quickly as possible to prevent further risks of diversion. We want everyone, both the government and the private sector, focused on prioritizing their enforcement and compliance resources to best protect our national security.

* * *

I mentioned at the beginning of my remarks that my father-in-law's jukebox is a 1947 Rock-Ola. If you're like me, maybe you assumed that whoever came up with the name "Rock-Ola" was playing off the type of music the jukeboxes became famous for – rock and roll. Perhaps you even thought the name was a mash up of "rock and roll" and "Victrola," one of the most popular record player manufacturers at the time. Turns out, the origin of Rock-Ola is a much simpler story. The man who founded the company back in 1927 (decades before the invention of rock and roll, by the way) was none other than David Rockola. He named the company after himself, simply inserting a hyphen between "Rock" and "Ola" so that people would pronounce it correctly.

But David Rockola didn't just start and run the company that bore his name. He also had direct experience with the cost-benefit calculus tied to making self-disclosures and making disclosures about the misconduct of others.

In the 1920s, David Rockola was the supplier of slot machines to an illegal syndicate run by Chicago organized crime. That is, until the authorities caught up with him. He was criminally charged with corruption, then given immunity in exchange for his cooperation against the Irish mob, including characters like James "High Pockets" O'Brien and Edward "Spike" O'Donnell. The evidence Rockola provided the prosecutors allowed them to indict 21 defendants for conspiracy, earning him a nickname himself – the "Crown Prince of the Slot Machine Syndicate." But when the time came for Rockola to testify at trial, he reversed course and refused to answer any questions. He was held in contempt of court and sentenced to six months in jail. Hat tip to the Made in Chicago Museum website for this piece of forgotten history.

Organized crime posed what seemed like an existential threat to the country in the 1920s. The power and influence of the Mob was formidable, and law enforcement often found itself both metaphorically and literally outgunned. Now, in the 2020s, the existential threat instead comes from nation-state actors, who are attempting to obtain our country's most advanced technologies in order to develop military capacities that can overwhelm ours. Just as we on the enforcement side have implemented policies and partnerships to ensure that our finite enforcement resources are best matched against these profound national security threats, we need companies to follow suit. We want you spending your compliance dollars on efforts that bring the greatest return on investment – that best prevent significant violations of our rules and thereby best help protect our national security.

Thank you.