When I last spoke at Update – my first – I had been the Assistant Secretary for Export Enforcement for about six months. During those six months, Russia had launched its full-scale invasion of Ukraine, and it felt like the pace and scope of changes to our export control rules were unrelenting. Nearly two years later, it still feels that way. Since I last spoke with you here, we’ve stood up the Disruptive Technology Strike Force, added hundreds of parties to the Entity List, strengthened our partnerships with our industry, interagency, and international counterparts, and brought charges against numerous illicit Russian, Chinese, and Iranian procurement networks. Given the global threat environment we currently face, our enforcement efforts have never been more central to America’s national security strategy.

But it’s not just practitioners and trade professionals like you that I speak to. A few months after speaking to all of you at the last Update, I returned to my hometown of Boston, Massachusetts, to speak to the current students at my former high school, Roxbury Latin. Talking with the faculty and students there, it was clear to me that Roxbury Latin’s overarching philosophy has remain unchanged – that character education is just as important as an academically rigorous one. The school, founded in 1645 and the oldest secondary school in continuous existence in North America, embraces distinct values and requires that its students live by them. As one example, the school is explicit about honesty being expected in all dealings. In fact, that’s the first fundamental standard listed in the school’s Handbook. When I was a student, Roxbury Latin’s then-Head, Tony Jarvis, reminded us every exam period that no grade was ever worth the price of our reputations. Cheating is not worth it.

Of course, it’s not just Roxbury Latin where this principle holds true. Taking a shortcut to finalize a sale is also not worth it. Profit cannot be the sole consideration. We need industry to prioritize compliance with our export rules – because the stakes have never been higher. According to the Annual Threat Assessment of the U.S. Intelligence Community released just a
few weeks ago, “An ambitious but anxious China, a confrontational Russia, some regional
powers, such as Iran, and more capable non-state actors are challenging longstanding rules of the
international system as well as U.S. primacy within it.” Our current geopolitical challenges, the
increasingly rapid development of technology with the potential to provide asymmetric military
advantage, and the countless ways in which the world is now interconnected have raised the
prominence and impact of export enforcement in unprecedented ways.

But we simply can’t succeed in our enforcement mission without your help. As Secretary
Raimondo has put it, “We need the private sector, including business, labor, and universities, to
work with us to ensure America’s long-term prosperity and security.” Effective compliance is
the first component of effective enforcement. It’s the compliance programs that you build that
identify and manage risk with new or existing customers, suppliers, and distributors. It’s the
time, money, and effort that you put into your compliance programs that stop sensitive U.S.
technology from going to our adversaries. It’s the Roxbury Latin ethos, albeit in a slightly
different context – it’s not worth prioritizing short-term profits over long-term reputational risk.
But the stakes here are much higher than those for cheating on a high-school exam. Failure to
prevent our adversaries from obtaining advanced U.S. technology carries not just significant
reputational risk for individual companies but also serious consequences for our collective
national security.

* * *

Since the last Update conference, we’ve announced a number of new policies and initiatives
designed to incentivize compliance and to promote effective enforcement. You’ll see this same
two-pronged strategy at work in each of our various announcements today. Our goal is to
encourage and incentivize investment in compliance on the front end, while also emphasizing the
financial and reputational cost of facing an enforcement action on the back end. In other words,
we need to ensure that the export laws are followed – because when they’re not, our national
security is harmed. We’re committed to implementing new and innovative ways to help
companies comply. And we’re equally committed to implementing more aggressive and
effective ways to hold companies that don’t comply accountable. Because the truth is that front-
end compliance and back-end enforcement are linked. Sometimes, for companies to be
convinced that it’s worth it to invest in compliance on the front end, they need a reminder of the
potential consequences of what can happen to them on the back end when they fail to make that
investment and they’re then facing a significant enforcement action.

Compliance on the front end

Let me tell you what we’ve done in the twenty-one months since the last Update conference.
Starting with front end compliance, we’ve conducted extensive outreach to educate industry and
academia about our policies and procedures, as well as the trends we’re seeing. With regard to
Russia, for example, we’ve published best practice guidance, including a sample end-use
certification form, for exporters to use to help prevent diversion of high-priority “battlefield
items,” like microelectronics and ball bearings, to the Russian war machine. We’ve also
conducted over 800 outreaches to the exporting community about the new restrictions.
More broadly, we’ve issued more than a dozen advisory notes, guidance documents, and alerts in coordination with other government agencies like the Departments of Justice, the Treasury, Homeland Security, and State. This unprecedented level of cooperation among different Cabinet agencies is designed to convey consistent and clear messaging about federal priorities on sanctions and export controls. Just a few weeks ago, for example, we published a tri-seal advisory with the Departments of Justice and the Treasury on the applicability of our respective controls and laws to non-U.S. entities. The advisory makes clear that parties outside the United States are not exempt from U.S. export controls or BIS enforcement when it comes to reexporting items subject to our regulations. We have also published multi-agency sealed documents on voluntary self-disclosures, the transfer of goods in the maritime environment, Russian evasion tactics, and Iran’s unmanned aerial vehicle-related (UAV) activities. In addition, we’ve issued joint alerts with the Financial Crimes Enforcement Network, or FinCEN, identifying evasion red flags and urging financial institutions to be vigilant against efforts by those who seek to evade export controls. All of these documents are available on our new and improved BIS website, and I encourage you to visit the site to review them.

We even published an industry advisory co-authored by the governments of five different allied countries – Canada, the United Kingdom, Australia, New Zealand, and the United States – that together comprise the “Export Enforcement Five,” or “E5,” a partnership committed to formal coordination on export enforcement. This “quint-seal” advisory, the first of its kind, amplifies the importance of the high-priority items that Russia is using in its weapons systems, as well as the need for companies to apply a risk-based approach to export compliance.

Many of these guidance documents stem from your feedback – from our meetings with industry, academia, exporters, trade associations, and others, who have asked questions about particular policies or trends we’ve identified. I’m sure we’ll get more questions, comments, and suggestions this week during Update. This feedback loop is critical so we can ensure that we’re doing our best to help you comply with our rules. Please keep the feedback coming.

For the academic community, we’ve gone a step beyond guidance documents. Over the last year, we expanded our Academic Outreach Initiative from 20 to 29 universities. The Initiative is designed to help academic institutions maintain an open, collaborative research environment in a way that also helps protect them from national security risk. Each partner university has an assigned outreach agent who has been meeting with the university quarterly to talk about new regulations, updates, and enforcement actions relevant to academia. We’ve also hosted webinars for the academic community on conducting open-source research, red flags specific to academia, and fundamental research.

In addition, we’ve updated our enforcement policies to help drive compliance, including our policies on voluntary self-disclosures (VSDs). Last April, we clarified our VSD policies with the goal of driving additional disclosures of significant possible violations of the Export Administration Regulations (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 award them future cooperation credit for doing so. These policies are working. Since their implementation, we’ve seen increases both in the number of VSDs involving potentially serious violations and in disclosures about the misconduct of others. Specifically, we received nearly 80% more VSDs containing potentially serious violations in FY2023 than we did in FY2022. And in the year since last April’s policy announcement, we’ve garnered approximately 20% more leads based on tips we received from industry than we did during the same time period for the preceding year.

More recently, in January, we reduced the administrative burden associated with submitting VSDs for more minor or technical violations. First, we encouraged companies to bundle minor or technical violations into a single overarching quarterly submission. Second, companies can now submit an abbreviated “narrative account” for minor or technical infractions. Prior to January’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. By simplifying the disclosure process for minor or technical violations, we’re encouraging companies to focus their resources on the more serious violations, where we continue to recommend a thorough review for the preceding five years.

Enforcement on the back end

At the end of the day, it’s up to all of you to build strong compliance programs and promote a culture of compliance within your respective companies or academic institutions. I’m hopeful our guidance documents, advisories, and best practices can help. But if you instead choose not to invest in compliance, you significantly increase your risk that an item will be unlawfully exported and that we will aggressively enforce. Mitigating national security risk costs money, one way or the other. We’d much prefer that you spend that money investing in compliance on the front end rather than paying it in fines on the back end. That way, you minimize the likelihood of harm – both to your reputation and to our national security. But either way, it’s going to cost something.

Lest you be tempted to dismiss this as just “tough talk,” last year saw our highest number ever of convictions, temporary denial orders (TDOs), and post-conviction denial orders. We also announced the largest standalone administrative penalty in BIS history – a $300 million penalty against Seagate Technologies to resolve allegations that Seagate shipped millions of hard disk drives to Huawei without a license in violation of the Huawei foreign direct product rule, or FDPR. We continue to use all of our tools – administrative, criminal, and regulatory – to hold violators accountable. In 2023 alone, our nominations resulted in more than 465 parties from China, Russia, Iran, and elsewhere being added to the Entity List through the established interagency process.

And you can expect our rapid enforcement tempo to continue. Since the last Update conference, we launched the Disruptive Technology Strike Force with the Department of Justice to protect a prioritized group of advanced technologies, such as artificial intelligence, from illegal acquisition and use by nation-state adversaries like Russia, China, and Iran. The Strike Force brings
together experienced agents and prosecutors in seventeen locations across the country. These agents and prosecutors are supported by an interagency analytical effort, comprised of analysts from BIS, FBI, HSI, and the Defense Criminal Investigative Service (DCIS).

In its first year, the Strike Force successfully charged 14 cases alleging sanctions and export control violations, smuggling conspiracies, and other offenses related to the unlawful transfer of sensitive technology to Russia, China, and Iran. In just the last month, two defendants pleaded guilty in two separate cases for their respective roles in running illicit procurement networks to supply the Russian military with U.S. microelectronics and other sensitive technologies. A few weeks ago, a Chinese national was indicted for allegedly trying to steal hundreds of confidential files containing artificial intelligence-related trade secrets from Google. Beyond the criminal cases, the Strike Force issued TDOs to cut off defendants’ access to controlled items and contributed to numerous parties being placed on the Entity List and the Treasury Department’s Specially Designated Nationals and Blocked Persons List.

Speaking of Treasury, our work has benefitted from leads generated out of Suspicious Activity Reports (SARs) filed with FinCEN. Whereas financial institutions previously had no systematic way to indicate suspected export control violations when filing SARs, FinCEN has now created two “key terms” for institutions to use – one for Russia diversion and one for export control evasion globally. To date, we have reviewed over 700 filed SARs, and we have been able to action more than 100 of those filings in various ways, including by sending leads to our enforcement agents, advancing existing cases, and developing Entity List packages.

We’ve also benefitted from our close relationships with our sister law enforcement agencies. Earlier this week, we signed a Memorandum of Understanding with HSI that formalizes our close coordination and partnership. We’re already lashed up tightly with HSI, given that we work nearly 40% of our major cases jointly with them. This MOU will ensure that this strong cooperation endures.

Internationally, our Export Control Officers continue their work to increase enforcement capacity across like-minded countries. We’ve enhanced collaboration with the Canada Border Services Agency by stationing a new Export Control Analyst in Ottawa and with the European Union’s (EU’s) Anti-Fraud Office, or OLAF, where our new data-sharing arrangement provides us visibility of how U.S. exports are moving through the 27 EU member states. From headquarters, we’re meeting monthly with our E5 and G7 partners to exchange information about Russian diversion tactics to identify end-use check targets and enforcement leads.

At the same time, our agents are working directly with their international enforcement counterparts. For example, our work with the Canadian authorities resulted in a criminal complaint unsealed in October charging three individuals in a multimillion-dollar global procurement scheme that sourced components used in UAVs and guided missile systems to sanctioned entities in Russia. Just last month, one of those individuals pleaded guilty to money laundering charges for her role in the scheme. Also last month, as a result of cooperation with
the Latvian authorities, a Latvian national pleaded guilty in the District of Connecticut for attempting to smuggle a jig grinder, which has defense and nuclear applications, from Connecticut to Russia. As part of that case, the Department of Justice transferred nearly $500,000 in forfeited Russian funds to Estonia, another crucial partner in the investigation, for the purpose of providing aid to Ukraine. This transfer was the first of its kind from the United States to a foreign ally for the express purpose of assisting Ukraine.

Since last Update, we’ve also enhanced our antiboycott enforcement efforts to ensure that U.S. companies are not used to support unsanctioned foreign boycotts, most notably the Arab League Boycott of Israel. In October 2022, we raised our penalties and instituted a requirement that companies entering into settlement agreements for antiboycott violations admit to a statement of facts outlining their conduct. Last July, we announced a renewed focus on foreign subsidiaries of U.S. companies and noted that we would explore additional ways to deter foreign parties from issuing or making boycott requests. We also modified the boycott reporting form to require submitters to indicate the identity of the requesting party.

These policy changes are bringing results. In the last year, we imposed over $425,000 in penalties on companies for alleged violations of the antiboycott regulations, including over $283,000 against Regal Beloit FZE, a foreign subsidiary of Regal Beloit America, Inc., to resolve 84 violations related to antiboycott requests from a Saudi Arabian customer.

As you can see, when things go sideways and items get wrongly exported, or when our antiboycott rules are violated, we will not hesitate to use all of our enforcement authorities. We’re also working internally to ensure that we’re using those authorities strategically to achieve the most impactful national security outcomes. At the start of the last 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, 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.

Again, we would much rather you comply with the export control rules on the front end. It’s better for you, since you don’t want your product found on the battlefield in Ukraine or your technology used by an authoritarian government to repress its population (both all too common real-world examples). And it’s better for us, because we don’t want your technology or product being used that way either.

Today, I’m announcing four new updates and policies to help further drive both front-end compliance and back-end enforcement. First, this morning, we published updated Freight Forwarder Guidance and Best Practices on our website. Over the past year, we met with trade associations, consolidators, and others within the global supply chain to discuss issues specific to the freight forwarding and express carrier communities. The updated guidance provides an overview of the roles, responsibilities, and best practices for freight forwarders in export
transactions. It includes red flags specific to freight forwarders and exporters, as well as a
discussion of how the antiboycott regulations apply.

Second, we’ve published on the new BIS website an updated version of “Don’t Let This Happen
to You,” our compendium of case examples highlighting our criminal and administrative
enforcement efforts. Don’t Let This Happen to You was last updated in October 2022, and as I
just mentioned, we’ve had a number of significant enforcement actions since then. As its title
implies, the publication provides useful illustrations of what not to do, of the type of conduct that
gets companies in trouble. We put this guide out because we mean it – we want to help make
sure you literally don’t let this happen to you. The case examples span the globe, from Michigan
to Singapore, as well as technology areas, from UAV and missile components to ghost guns.

Third, as I mentioned earlier, we modified the boycott reporting form last year and now require
those reporting boycott requests to list not just the requesting country but also the identity of the
actual requesting party. With this modification to the form, we’ve been able to compile a list of
entities who have been identified in these reports as having made a boycott-related request.
Today, we are publishing that list on our website as a resource for companies, financial
institutions, freight forwarders, and others. We want to help you comply with our antiboycott
regulations. By publishing this list, we aim to raise awareness of the sources of past boycott
requests, facilitate fulfillment of the antiboycott reporting requirements, and deter foreign parties
from imposing – and U.S. parties from acquiescing to – boycott-related requests and conditions.
We encourage you to diligently review transaction documents from all sources, but especially
transaction documents with these parties, given that they’ve been identified by others as a source
of boycott requests.

And fourth, we’re taking additional steps to help combat the shipment of Western components
into Russia, where they’re being used in missiles and drones. We heard directly from non-
governmental organizations (NGOs), trade associations, and semiconductor companies that they
wanted more information to help them identify Russian front companies in third countries. So
last year, we initiated an effort to identify customers of U.S. companies and distributors within
supply chains that were continuing to ship high-priority items to Russia. We then sent the U.S.
companies “red flag” letters identifying specific customers of theirs who had been identified in
customs data as continuing to export to Russia. We encouraged the companies receiving those
letters both to use heightened due diligence for their identified customers and to further augment
their export screening efforts by purchasing commercially available datasets of Russian imports
and screening against them as well.

We’ve now gone further and are sending information from these commercially available datasets
directly to the U.S. manufacturers and distributors who make and sell products that continue to
be found in recovered missiles and drones inside Ukraine. The datasets list parties in third
countries that have continued to sell dual-use items to Russia. In the last several weeks, we’ve
sent letters to more than 20 American companies, each containing a list of more than 600 foreign
parties identified in the datasets. In those letters, we’ve requested that the American companies
voluntarily stop shipping to these parties due to the high risk of transshipment to Russia. That’s
in addition to the work our Under Secretary has been doing with his counterparts from the
Departments of State and the Treasury – reaching out directly to senior leaders at U.S.
companies to discuss further steps they can take to help prevent their products from ending up inside Russian weapons.

For the sake of the people of Ukraine and a world order that stands against nation-state aggressors, we must continue to work as closely as possible with industry, our interagency colleagues, and our international partners. That way, we can both impede the Russian war machine and deter other would-be aggressors from following Putin’s path.

* * *

I mentioned at the outset that my high school, Roxbury Latin, was founded in 1645. If you’re doing the math, that means my high school is older than our country. A Roxbury Latin alumnus, General Joseph Warren, was actually the person responsible for sending Paul Revere and Samuel Dawes on their famous midnight ride to warn the colonists in Concord and Lexington that the British were coming. Joseph Warren died two months later, killed in one of the most famous battles of the Revolutionary War, the Battle of Bunker Hill. A statue in his honor stands on the Roxbury Latin campus.

In their own way, export controls played a role in the Revolutionary War as well. Just a few months after the Boston Tea Party in December 1773, Joseph Warren and his fellow Boston Town Meeting members passed a resolution calling for an economic boycott of Great Britain in response to the British barricade of Boston Harbor. Later that year, the first Continental Congress adopted the Articles of Association, which called for a trade boycott against not only British imports but also exports by the colonists. It was understood, even then, just how critical economic sanctions and export controls are as a tool of foreign policy. As the Boston Town Meeting resolution stated, if Great Britain were to continue its “exports and imports, there is high reason to fear that fraud, power, and the most odious oppression, will rise triumphant over right, justice, social happiness, and freedom.”

Our policies and initiatives over the past few years, from the issuance of high-priority item supplier lists to updates to our voluntary self-disclosure procedures, have all been designed to promote compliance on the front end and, if that fails, strengthen enforcement on the back end. We’re operating in a fundamentally different strategic environment from even a decade ago, let alone the 1700s. The decisions you make today on where and how you undertake research, engage in trade, and make investment decisions will profoundly shape our economic and national security for decades to come. While we no longer fear the arrival of the British (since they are now among our closest allies), we need to be more vigilant than ever against today’s adversaries, the ones who are now “coming” for us. We need everyone – law enforcement, industry, and academia – working together to protect American technology from them.

Thank you.