

**ADVANCING NATIONAL SECURITY AND FOREIGN
POLICY THROUGH EXPORT CONTROLS: OVER-
SIGHT OF THE BUREAU OF INDUSTRY AND
SECURITY**

HEARING
BEFORE THE
COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE ACTIONS TAKEN BY THE BUREAU OF INDUSTRY AND
SECURITY, INCLUDING THOSE TAKEN TO RESPOND TO RUSSIA'S FUR-
THER INVASION OF UKRAINE, ENGAGE WITH INTERNATIONAL ALLIES
AND PARTNERS ON EXPORT CONTROLS, ADDRESS HUMAN RIGHTS
VIOLATIONS, AND ENFORCE EXPORT CONTROLS

JULY 14, 2022

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

SHERROD BROWN, Ohio, *Chairman*

JACK REED, Rhode Island	PATRICK J. TOOMEY, Pennsylvania
ROBERT MENENDEZ, New Jersey	RICHARD C. SHELBY, Alabama
JON TESTER, Montana	MIKE CRAPO, Idaho
MARK R. WARNER, Virginia	TIM SCOTT, South Carolina
ELIZABETH WARREN, Massachusetts	MIKE ROUNDS, South Dakota
CHRIS VAN HOLLEN, Maryland	THOM TILLIS, North Carolina
CATHERINE CORTEZ MASTO, Nevada	JOHN KENNEDY, Louisiana
TINA SMITH, Minnesota	BILL HAGERTY, Tennessee
KYRSTEN SINEMA, Arizona	CYNTHIA LUMMIS, Wyoming
JON OSSOFF, Georgia	JERRY MORAN, Kansas
RAPHAEL WARNOCK, Georgia	KEVIN CRAMER, North Dakota
	STEVE DAINES, Montana

LAURA SWANSON, *Staff Director*

BRAD GRANTZ, *Republican Staff Director*

ELISHA TUKU, *Chief Counsel*

DAN SULLIVAN, *Republican Chief Counsel*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

PAT LALLY, *Hearing Clerk*

C O N T E N T S

THURSDAY, JULY 14, 2022

	Page
Opening statement of Chairman Brown	1
Prepared statement	24
Opening statements, comments, or prepared statements of:	
Senator Toomey	3
Prepared statement	25

WITNESS

Alan F. Estevez, Under Secretary for Industry and Security, U.S. Department of Commerce	5
Prepared statement	26
Responses to written questions of:	
Chairman Brown	32
Senator Warren	33
Senator Tillis	36

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Letter submitted by The Bureau of Industry and Security	38
---------------------------------------------------------------	----

ADVANCING NATIONAL SECURITY AND FOREIGN POLICY THROUGH EXPORT CONTROLS: OVERSIGHT OF THE BUREAU OF INDUSTRY AND SECURITY

THURSDAY, JULY 14, 2022

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:01 a.m., in room SD-538, Dirksen Senate Office Building, Hon. Sherrod Brown, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN SHERROD BROWN

Chairman BROWN. The Committee on Banking, Housing, and Urban Affairs will come to order. We welcome our witness, Alan Estevez, who serves as Under Secretary for Industry and Security at the Department of Commerce.

I thank Ranking Member Toomey and his staff for their help in confirming Under Secretary Estevez and the two Assistant Secretaries at the Bureau of Industry and Security: Thea Kendler for Export Administration and Matt Axelrod for Export Enforcement. That is important as other confirmations in the Federal Reserve and others have been.

This is the first time since we passed the Export Control Reform Act in 2018 that Congress has fully confirmed the full BIS leadership.

Because of this Committee's work, for the first time since 2013, close to a decade, we have a full, confirmed Federal Reserve Board. It is our job to do these things.

We have confirmed, as I just spoke with the Under Secretary a moment ago, a fourth member of the Ex-Im Board. We have a fully functioning Export-Import Bank, also important.

And for the first time in our history, these nominees are beginning to look more like America in terms of gender and race and background and diversity generally.

The world changed on February 24th when Russia invaded Ukraine, continuing—I would underscore “continuing”—its barbaric war on the Ukrainian people and their sovereignty.

Vladimir Putin has been shocked by two things: the strength of the Ukrainian resistance; and the skill of this President in assembling and uniting a broad coalition, the likes of which we have not seen in decades. Think about this: Germany, Finland, Sweden, Switzerland.

We have isolated Russia. We have limited its ability to access the tools and technologies it needs to continue its grotesque, immoral, inhumane war against Ukraine.

BIS has been integral in our international response to siphon off Russia's access to military material. I thank all of you for that. It quickly rolled out a sweeping series of rules designed to stall and degrade Russia's military and technological capabilities.

BIS targeted Russia's defense, aerospace, and maritime sectors. It applied controls to U.S. exports and to items produced abroad that use U.S. software, U.S. technology, or U.S. equipment.

Since February 24th, BIS has issued a dozen new rules, ramped up enforcement activity, and continued to build what Assistant Secretary Axelrod called "the broadest expansion of multilateral export controls among like-minded partners since the creation of CoCom back in cold war days in 1949."

The results have been impressive.

Exports to Russia by countries who have imposed sanctions have fallen 60 percent.

At the same time BIS weakened Russia's military, it committed to ensuring that those items that benefit the Russian people, like medical supplies, are still available.

This ability to distinguish bad actors—whether they are State or non-State actors—while still allowing innocent civilians to benefit from U.S. exports is crucial, threading that needle is crucial, as the agency builds on this international coalition to address other national security and foreign policy challenges.

To that end, Mr. Under Secretary, I am encouraged by your statements calling for strengthening or supplementing our existing multilateral regimes.

Enhancing our multilateral regimes requires patience—by BIS and by Congress. We must work with allies to identify the items and the technologies that present a risk to our collective national security.

It is important work. I am pleased to hear that it is one of Under Secretary Estevez's top priorities.

Back in 2018, when this Committee worked to enact the Export Control Reform Act, we included policy statements, guiding BIS in developing export control policy.

One of these guiding principles is that our national security requires that the U.S. maintain our leadership in science, technology, engineering, and manufacturing.

That value should guide our export control policy. It should guide our work in Congress.

We do not want to be at the mercy of our competitors—or our adversaries—for technology and other inputs vital to a 21st century economy. Dependency on countries like China poses a huge economic risk and an unacceptable national security risk.

It is why we need investments in research and development and investments in our fellow citizens.

We have an innovation and competition bill in conference that would do just that. I appreciate Mr. Estevez's enthusiastic support for that bill.

Ranking Member Toomey and his staff—and I compliment them—have worked in good faith with me and my staff to negotiate

this Committee's conference provisions. I thank them for that important work.

We have reached bipartisan agreements on provisions with the House Foreign Affairs Committee and the House Financial Services Committee.

It is time for us to vote on and pass a final bill that promotes U.S. science, U.S. technology, and U.S. manufacturing so we maintain U.S. economic leadership.

This bill will create thousands, likely tens of thousands of good-paying jobs in Ohio and many more around the country—jobs in growing industries, jobs where you build careers. In my State, those 10,000 jobs, at least 10,000 jobs, are at stake. Business leaders and labor leaders are desperate for this investment.

The head of the Ohio Chamber of Commerce and my friend, former Congressman Steve Stivers, and the head of the Ohio Business Roundtable, former Republican Congressman Pat Tiberi, have been particularly vocal about this support.

We must act now.

For decades—we know this. For decades, at the behest of corporate America, policymakers of both parties have passed bad tax policy and bad trade policy that not only allowed but really encouraged these companies to move jobs overseas and supply chains and technology abroad—always in search of lower wages, always in search of weaker worker protections, always in support and encouraging low-level environmental enforcement. And when the production moves abroad, innovation moves with it. And then we act surprised.

We invented semiconductor chips. Ninety percent of them are now made overseas, again, because of a corporate trade policy that far too many Members of this Senate and House acquiesced in when faced with intense corporate lobbying.

We have to fix that now. This is our chance.

Americans have waited long enough. We should pass this bill this month.

If Congress is serious, if we are serious about the threats that face us, regardless of the politics, it must be similarly serious about supporting American innovation.

Senator Toomey.

OPENING STATEMENT OF SENATOR PATRICK J. TOOMEY

Senator TOOMEY. Thank you, Mr. Chairman. And, Under Secretary Estevez, welcome.

The Bureau of Industry and Security, or BIS, determines which U.S. goods are too sensitive to be shipped abroad. In the face of China's drive for dominance in key tech sectors especially, BIS' mission today is as important as it has ever been. By setting U.S. export control policy on items used for both civilian and military purposes, BIS effectively has the power to reshape the supply chains of entire industries. That means BIS must craft export controls in a prudent, thoughtful, and effective manner that advances U.S. national security interests without unduly harming American economic interests.

The issue I would like to focus on today is a legislative concept that has received a growing amount of attention in recent months.

It falls entirely in the jurisdiction of this Committee, and it would unquestionably impact BIS' mission and work flow if enacted. I am referring to a concept known as "outbound CFIUS."

The idea of outbound CFIUS is to establish a new agency within the Executive branch and to give this agency vast, potentially unchecked authority to regulate, intervene in, and even block all kinds of potential activities, including prohibiting Americans and U.S. firms from investing in, selling to, or buying from companies in certain countries, most notably China.

Outbound CFIUS could also provide the President with extremely broad authority to determine which industries are subject to regulation of this sort. And it is not just semiconductor firms that we would be talking about. Any industry determined to be in the national security interest of the United States could be impacted.

President Biden's recent invocation of the Defense Production Act for baby formula is just the latest reminder of how the Executive branch can abuse the term "national security."

President Trump also abused the notion of national security, having the Commerce Department laughably assert in a 232 investigation that the import of foreign cars was somehow a threat to our national security.

Now, it appears that Mr. Estevez perhaps agrees with this because, during his confirmation hearing before this Committee, he said to me, and I quote: "232 is an important tool. Section 232 needs to be looked at in a hard national security lens, Senator. It should not be used willy-nilly."

I share Mr. Estevez's concern about national security authorities being abused by any President willy-nilly. It is not an overstatement to suggest that hundreds or thousands of U.S. companies and tens if not hundreds of billions of dollars in commerce could be impacted by outbound CFIUS.

The rise of China presents the United States with the greatest security challenge we have faced since the end of the cold war. I am very clear-eyed about the fact that the Chinese Communist Party has embarked on a concerted, whole-of-Government campaign to surpass the technological leadership of the United States in the areas that will underpin geopolitical, military, and economic power for decades to come, all to further their ambition to displace America as the world's dominant superpower.

But how we address this challenge matters. Doing outbound CFIUS and getting it wrong could actually impede national security, including the work of security agencies such as BIS or CFIUS that are already doing important work with respect to China. Getting it wrong could also severely harm the United States. We cannot prevail in this contest with China by emulating China, like the China competition bill before the Senate envisions in many ways.

Instead, we need to out-innovate China and protect our intellectual property from theft and illicit transfer. That means ensuring that the United States remains the single greatest global destination for capital formation, research and development projects, and the smartest minds in the world to come and work. Getting outbound CFIUS wrong puts all of this into jeopardy by

disincentivizing the flow of capital, ideas, and people to come to the United States.

There are many important questions about outbound CFIUS that remain to be answered. For example, what exactly is the problem outbound CFIUS is attempting to solve? How do current laws and authorities such as export controls address or fall short of addressing these problems? How would outbound CFIUS affect the United States as a destination for capital formation and technological innovation?

Now, I am not the only one concerned about the reasoning and implications of standing up an outbound CFIUS mechanism. I have here, Mr. Chairman, a letter from three former officials from the last Administration who directly oversaw CFIUS and export controls. The letter raises concerns about the scope and justification for outbound CFIUS and calls for any such mechanism to be grounded in a clear, statutory law brought about through regular order. Mr. Estevez's predecessors clearly are concerned about the way in which outbound CFIUS is laying out. I think he should be concerned, too.

In addition, 11 trade associations representing hundreds of companies and thousands and thousands of workers sent a letter to Congress expressing opposition to the inclusion of outbound CFIUS in the China competition bills that are under consideration. I ask that these two letters be entered into the record.

Chairman BROWN. Without objection, so ordered.

Senator TOOMEY. So given these concerns, I think Congress really has to take the time to properly evaluate the outbound CFIUS concept rather than rushing to enact legislation that is not properly vetted.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

I appreciate the Ranking Member's comments about the outbound investment provisions. I meant what I said in my opening statement. I want to pass a final competition bill this month. Time is up. We need to act. I will work with my colleagues on this issue, but we should do so in another vehicle. So, Pat, thank you.

It is my pleasure to welcome Under Secretary of Commerce Alan Estevez. He was sworn in in early April. Thank you for joining us. You are recognized for your testimony.

**STATEMENT OF ALAN F. ESTEVEZ, UNDER SECRETARY FOR
INDUSTRY AND SECURITY, U.S. DEPARTMENT OF COMMERCE**

Mr. ESTEVEZ. Thank you, Chairman Brown, thank you, Ranking Member Toomey, and thank you, Members of this Committee, for inviting me to testify before you today on the work of the Commerce Department's Bureau of Industry and Security, or BIS.

As the Under Secretary of Commerce for Industry and Security, I view my role as the Chief Technology Protection Officer of the United States. Our primary goal is to prevent malign actors from obtaining or diverting technologies that can be used against the United States or its allies in order to protect our national security and advance our foreign policy objectives.

Export controls are a unique and powerful tool for responding in the modern environment. This is particularly true when we work together with our allies and partners.

Today I will briefly discuss BIS' role in administering and enforcing export controls in response to Russia's further invasion of Ukraine; the pacing threat of China; the identification of emerging and foundational technologies essential to national security; and building a durable, multilateral technology security framework for export controls.

Since February 24th, we have imposed sweeping export controls on Russia for its unjustified, unprovoked, and premeditated invasion of Ukraine and on Belarus for its substantial enabling of that invasion. I want to thank the Members of this Committee for their support for additional funding for BIS in the first Ukraine supplemental spending bill that passed in March.

We are choking off exports of technologies and other items that support Russia's defense, aerospace, and maritime sectors and are degrading Russia's military capabilities and ability to project power. For example, overall U.S. exports to Russia have decreased approximately 88 percent by value since last year, and other countries implementing similar controls have seen export decreases around 60 percent.

Importantly, since our controls have fully taken effect, worldwide shipments of semiconductors to Russia have dropped 74 percent by value compared with the same period in 2021. Also, reports indicate Russia will have to ground half to two-thirds of its commercial aircraft fleet by 2025 in order to cannibalize them for parts due to the controls we have implemented. This is one of the most aggressive and robust uses of export controls against another country, and the effects would not be possible without the coalition of 37 other countries so far that have adopted substantially similar controls on Russia and Belarus.

As we continue our robust response to Russia's invasion of Ukraine, we remain focused on aggressively and appropriately using our tools to contend with the long-term strategic competition with China. My North Star at BIS is to ensure we are doing everything within our power to prevent sensitive technologies with military applications from getting into the hands of China's military, intelligence, and security services.

BIS maintains comprehensive controls against China, including for the most sensitive items under our jurisdiction, as well as for predominantly commercial items when intended for military end uses or end users in China.

As part of our controls, we have nearly 600 Chinese entities on our entity list, 107 of those added during the Biden administration. China remains a complex challenge in the competition between democracies and autocracies. We are closely reviewing our approach to China, seeking to maximize the effectiveness of our controls.

Another part of our mission at BIS is to identify and impose appropriate controls on emerging and foundational technologies essential to national security. Since enactment of this statutory requirement, BIS has established 38 new controls on emerging technologies, including controls related to semiconductors, bio-

technology, and quantum computing. I continue to prioritize this issue.

As part of this important mission, I have asked the Department of Defense Under Secretaries for Acquisition and Sustainment and for Research and Engineering to work with me to establish a critical technologies review board. This board will help BIS to understand the technologies DOD is investing in for military use and help us impose appropriate controls for those technologies.

For the United States to maintain effective export controls and technology leadership, we need to coordinate with others. Our work with 37 other countries to implement the Russia controls helps provide a blueprint for further progress. We need to work with our allies to develop a 21st century export control framework for the digital age, which includes working with like-minded suppliers of sensitive technologies as well as addressing the use of commercial technologies to commit human rights abuses.

Finally, enforcement is critical to ensuring effective export controls, and we are working with partners across the globe to enhance export control enforcement. I value the collaboration and partnership with this Committee as we tackle national security challenges together.

Thank you again for inviting me here today to testify, and I look forward to your questions.

Chairman BROWN. Thank you, Mr. Under Secretary.

The questioning will begin with the Senator from Nevada, Senator Cortez Masto, for 5 minutes.

Senator CORTEZ MASTO. Thank you, Mr. Chairman.

Chairman BROWN. Of course.

Senator CORTEZ MASTO. I appreciate the consideration.

Under Secretary, in May, the Bureau of Industry and Security announced its decision, as we have been talking about, to cease which technologies subject to new export control under the Export Control Reform Act are either emerging or are foundational and instead identify all such technologies together as Section 1758 technologies. So can you elaborate on how the Bureau expects this change to speed up efforts to identify technologies significant to U.S. national security?

Mr. ESTEVEZ. Thank you for that question, Senator. We found going through the process, while we were looking at emerging and foundational technologies, an interagency debate over what is the difference between emerging and foundational. For example, is a 5 nanometer semiconductor emerging technology or is it foundational, a next generation of an existing technology? Is a Tesla a new emerging vehicle, or is it just a car?

So instead of dancing around that, to get technology protections out, we wanted to just identify them within the statute, number 1758. That does not mean we will not go back and identify them as emerging or foundational and put appropriate controls. My guiding light is to put appropriate controls on technologies that may threaten the United States if used by the wrong people. But to get through the interagency process, we are going to blur that distinction.

Senator CORTEZ MASTO. So could this lead to a rise in designations of such technologies and an increase in mandatory filings

with CFIUS? Would this add more bureaucracy and slow this process down somehow, impeding our national security in being able to identify these technologies?

Mr. ESTEVEZ. I do not believe so, Senator. I am a former DOD rep to CFIUS for 6 years. CFIUS needs to look at technologies for investment, including passive investment, under the rules of FIRMA. They can do that using broad categories of technologies—AI, quantum computing. To do an export control, I need a more definitive identification of that technology. What is the algorithm? Which CFIUS does not need. CFIUS needs to look at a broader scope.

So, for me, this is an easier way to get the proper controls around technologies that could be used against us while still allowing the processes to work.

Senator CORTEZ MASTO. Thank you. And we talked about this. China is the greatest long-term threat to the United States and democracies around the world with their economy and at so many other levels, and it has a clear plan to use all forms of their Government, their economy, their military, the industry, to really gain that competitive advantage over the United States.

My question to you, Under Secretary, is: What additional authorities—tell us as you are here today—or resources do you need in order to address this threat that is posed by the Chinese Government?

Mr. ESTEVEZ. I think I have the proper authorities under ECRA, so I do not believe I am missing any authorities. I would be remiss since you asked the question about resources—look, you know, BIS is a fairly small organization. I could always use more technologists, more enforcement officers, you know, and a larger budget to use some tools that can give us access to supply chain mapping, for example. You know, so I would always look to Congress to help me in that regard.

Senator CORTEZ MASTO. So let us talk about that workforce, though. Does that workforce exist? Do we have the skill set for what you need to be able to hire?

Mr. ESTEVEZ. I have some fantastic technologists on my staff. I think the talent is out there. Obviously, Government has to compete for that talent with the private sector. But, you know, there are people like me who came back from the private sector who want to do the right thing to protect our national security, and I think we can access that talent.

Senator CORTEZ MASTO. Thank you. And then, finally, how is BIS working to protect the U.S. IP and innovation with the interagency to ensure that critical and emerging technologies do not land in the hands of our adversaries such as Iran and North Korea?

Mr. ESTEVEZ. So just like our protections against China and China's theft of IP, you know, we would have the same kind of controls. Theft of IP is a violation of export control, because we also control the technical data around specific technologies. So if we found that someone that we could pinpoint that was stealing IP, that person/entity would probably land on the entity list, and we would take appropriate actions with our interagency partners.

Senator CORTEZ MASTO. Thank you. Thank you, Mr. Under Secretary, for joining us today.

Chairman BROWN. Thank you, Senator Cortez Masto.

Senator Toomey is recognized.

Senator TOOMEY. Thank you, Mr. Chairman.

Mr. Estevez, I just wanted to sort of try to establish some baselines here. First of all, I trust you would agree that any technology transfer, even as part of an outbound investment by an American firm into China, is currently subject to existing export controls.

Mr. ESTEVEZ. Yes, I would, Senator.

Senator TOOMEY. OK. So BIS, as I think you just said, has the authority to block the transfer of really any kind of technology, intellectual property, blueprint, procedural know-how, software, and that does not end because a U.S. company has entered into, say, a joint venture with a Chinese company.

Mr. ESTEVEZ. That is correct. They would need a license if it was a protected technology.

Senator TOOMEY. Right. So let me just drill down on this and make it very clear. If an American venture capital firm, for instance, is investing in a Chinese artificial intelligence company that has ties to the Chinese military, a technology transfer that is associated with that deal that included some kind of intellectual property or sensitive blueprints or services or procedural know-how, none of that escapes the jurisdiction of these export controls because it is part of an investment deal.

Mr. ESTEVEZ. If there was a technology transfer as part of that investment, that is correct, Senator.

Senator TOOMEY. Right. So, likewise, if an American semiconductor firm, software firm, has a joint venture with a Chinese company, the Chinese company cannot just get, again, the sensitive technology, intellectual property, or any of that; they do not come out from under the export control.

Mr. ESTEVEZ. That is correct. It is a slippery slope once you start working with companies.

Senator TOOMEY. So I guess the question becomes: Is it your view that the BIS has sufficient authority to control the transfers of sensitive American technology to China?

Mr. ESTEVEZ. Yes, Senator, BIS has the appropriate controls to protect transfer of technology.

Senator TOOMEY. OK. So you have got that authority. But I think you have said that you think we still, nevertheless, need to have some kind of outbound investment review mechanism, even though you have just said we already have the authorities to prevent any kind of technology transfer. So I think given the limitations on time, I am going to not ask you to explain fully how and why we need to have that limitation on investment when you have said we already have the full authority to prevent the technology transfer.

I guess what I would like to ask you is this: I think we all know that when Congress passed ECRA, we did not intend for that law to contemplate a regime to regulate and block investment. So if we are going to stand up a regime that empowers that, don't you think that that ought to happen as a result of specific new statutory action by Congress?

Mr. ESTEVEZ. I agree there should be statutory action.

Senator TOOMEY. OK. So we should pass a law. And that comes completely under the jurisdiction of the Banking Committee, so the sensible way forward would be to have hearings on this to understand the need for this. I would like to have you back for an occasion where you could explain why you think we need this given that you have already said we have full capability to block technology transfer. I assume you would support and work with this

Committee on that.

Mr. ESTEVEZ. As you know, Senator, I would always come before this Committee if asked.

Senator TOOMEY. Let me ask you this: If a foreign company violates our export controls, is that sufficient grounds for putting that company on the entity list?

Mr. ESTEVEZ. If a foreign company violates our export controls, that is a likely—they would be a likely candidate for an entity list listing.

Senator TOOMEY. Likely candidate, so—

Mr. ESTEVEZ. Yes, I would put them on the entity list.

Senator TOOMEY. OK. All right. OK. Now, last year, China conducted two hypersonic missile tests which the Chairman of the Joint Chiefs, General Mark Milley, described as being very close to a Sputnik moment for the United States. There is also growing speculation that China will soon unveil its H-20 nuclear-capable stealth bomber.

Several months ago, my staff and the staff of the Chairman requested a briefing on the hypersonic test to hear from BIS an assessment of whether or not and to what extent any U.S. technology that was used in the development of that system, but we have not yet received that briefing. So I would like now to expand that briefing to include an analysis of whether U.S. technology of any sort has been involved in the development of the H-20 bomber. Can you commit today to give us that briefing within the next month?

Mr. ESTEVEZ. I will commit to give the Committee what Commerce can give. The reality is that is a much more complex problem that involves other agencies, including—

Senator TOOMEY. But we have not had the BIS briefing.

Mr. ESTEVEZ. I am happy, Senator, to give what BIS has.

Senator TOOMEY. And we can do that within a month?

Mr. ESTEVEZ. Yes, sir.

Senator TOOMEY. All right. Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Toomey.

Senator Tester from Montana is recognized from his office.

Senator TESTER. Thanks for being here, Mr. Estevez. I serve as Chair of the Defense Appropriations Subcommittee, and there has been a lot of talk about national security, and rightfully so, as it applies to your agency. Just on a side note, if we really want—if we are really concerned about national security, we as a Senate need to put politics in the back pocket for once in our lives and make sure we get USICA passed and make sure that we get our appropriations bills done by the end of this fiscal year, which is our job. And if we do not do that, then we are putting everything at risk that we stand for as a Nation. And I think now is not a time to play games or extend to a CR for even 30 days. The fact is that

if we are going to have, in my case, a Defense Department that works, if we are going to have domestic programs that work for this Nation, these budgets need to be out by the end of September and no more screwing around. We need to do it. And I would hope that everybody on this Committee pressure their leadership and the Chairman and Ranking Member of the Appropriations Committee to do exactly that.

I want to talk to you, Mr. Estevez, about exports to Ukraine to fight back against the Russian invasion. Do you have a system in place to expedite the consideration of those exports?

Mr. ESTEVEZ. We do, Senator.

Senator TESTER. Could you walk me through what that process looks like, what that approval process looks like?

Mr. ESTEVEZ. So like all—

Senator TESTER. As briefly as you can.

Mr. ESTEVEZ. Like all licenses that may require—or items that are exported that may require a license, it goes through the inter-agency process. But we would move them up to the top of the list in order to make sure that we are providing the Ukrainian military the capability they need to defeat the Russians.

Senator TESTER. And so what kind of timeframe do you look at for those approvals?

Mr. ESTEVEZ. They are going within weeks, Senator, or shorter.

Senator TESTER. So there has been much said about China, and rightfully so, because there is a lot to be said about what China is doing. The technology that we are giving the Ukrainians, I do not want to get into what that is at all. But the truth is that anything we give Ukraine, you have got to assume China can get. How do you accommodate that?

Mr. ESTEVEZ. So our export controls that I control are over dual-use items, not the military equipment that the Department of Defense is providing to China—excuse me, providing to Ukraine. And, you know, none of the items that we are talking about are like the type of high-end tech that we are looking at protections around China.

Senator TESTER. OK. You prefaced that by saying not the military stuff. What about the military stuff? You have oversight over that also.

Mr. ESTEVEZ. I do not have oversight over the provision of military equipment. That is under the jurisdiction of the State Department.

Senator TESTER. What about the technology that goes with that military equipment? Still part of the State Department?

Mr. ESTEVEZ. If it is embedded inside like a HIMARS Unit, for example, or an M777, which is an artillery piece, that is under the jurisdiction of State.

Senator TESTER. Do you have any concern about State's ability to be able to keep valuable information out of the hands of Russians and the Chinese?

Mr. ESTEVEZ. It is a matter of what is captured on the battlefield, I guess is what you would be concerned about.

Senator TESTER. That is correct.

Mr. ESTEVEZ. Nothing that I am aware of—and I am not, you know, playing in the Department of Defense's role of providing

equipment. But I am familiar with the equipment that they have provided. None of that equipment is what I would call our crown jewels.

Senator TESTER. OK.

Mr. ESTEVEZ. Because the Ukrainians are not capable of using that equipment, quite frankly.

Senator TESTER. I have got you. The last time we had one of these hearings in 2019, there was no one from the Administration to testify. I was frustrated by that then, so I just want to thank you for being here, because export controls are really very important to our national security, and Congress has a responsibility to provide the oversight of how that is working, and a great way to do that is to have folks like you in front of this Committee. So balancing our national security with export competitiveness is also really, really, really important.

In your role, how do you ensure that that is happening at BIS?

Mr. ESTEVEZ. Through our interagency licensing process. It is not just me that looks at stuff. It is the Department of State, Department of Defense, Department of Energy for all licenses. So that process in and of itself has a good divergence of views, you know, that usually come together in a coordinated fashion, and I think we—I personally believe that we need to balance those authorities.

With that said, I also believe we do need to prevent the most sensitive technologies from going to people who have identified that they would like to use it against us.

Senator TESTER. Thank you. Thank you, Mr. Chairman, and thank you, Mr. Estevez.

Mr. ESTEVEZ. Thank you, Senator.

Chairman BROWN. Thank you, Senator Tester.

Senator Daines of Montana is recognized.

Senator DAINES. Mr. Chairman, thank you, and thank you for coming to the Committee today. The United States is facing serious shortages of semiconductors, used in virtually every aspect of our economy. I believe this is truly becoming a national security concern. Whether it is health care, whether it is the military, semiconductors form the core of our modern economy. I believe it is critical that we dramatically increase domestic manufacturing as well as the fabrication of semiconductors and ramp up our enforcement of intellectual property violations by China. And I believe the Senate version of USICA does just that, and they do through the important CHIPS funding and also with the addition of my bipartisan Protecting IP Act. I believe it is critical that our colleagues across the aisle abandon their partisan tax-and-spend proposals and that Congress focuses on this very real national security threat by passing the bipartisan Senate USICA bill.

However, BIS can be doing more right now, I believe, with their existing authorities. It is clear that China is seeking to leapfrog semiconductor technology by stealing American IP, and companies that are supposed to be on your entity list are still finding a way to access American intellectual property.

So here is my question: What is BIS doing to ensure that high-tech and national security IP is not ending up in the hands of the Chinese Government?

Mr. ESTEVEZ. Thank you for that question. That is frankly what I spend my sleeping and waking hours thinking about, Senator. Now, we do have some cutoff points at the most sensitive highest tech semiconductors and the tooling that would make those semiconductors being allowed to be exported to China, so there is a cutoff point. I am conducting a complete review over those policies within BIS right now, and then there is also an interagency process looking at this. So there is a red line on what we would allow the Chinese to access.

With regard to listing folks on the entity list, you know, I cannot talk about any existing investigations that we may have, but we are always looking at all sources of data, open source, input from, you know, articles from think tanks, and certainly classified information on what Chinese firms may be doing. You know, we do have a legal process that is interagency to do that, and I always want to make sure that I have the legal standing to get someone on the entity list that, if they happen to sue us, we win.

Senator DAINES. Mr. Estevez, how much time have you spent in China before you served in this capacity?

Mr. ESTEVEZ. Zero.

Senator DAINES. Never been there?

Mr. ESTEVEZ. Never been there, partly because, you know, my whole career has been with the Department of Defense.

Senator DAINES. Whereabouts in the region have you traveled outside of China?

Mr. ESTEVEZ. I have been to Japan, Korea.

Senator DAINES. I lived in China for 6 years, worked for Proctor & Gamble, had two kids born in Hong Kong, and one of the things I have—one of my missions serving the U.S. Senate is to take U.S. Senators—this is pre-COVID—into China and to see it. And the supply chain issues are very, very critical, but equally critical and perhaps even a greater threat is the innovation ecosystem that China is building, STEM graduation rates, you know, ten times greater than the United States of America. They are building not only in terms of the scale of the innovation ecosystem, but now the quality of the IP that they can generate. So it is about stealing IP, but it is now shifting increasingly to generating IP. And I think this is one of the greatest threats we face as a Nation over the course of the next several decades.

Mr. ESTEVEZ. Senator, I agree that they have an incredible ecosystem. I would put our ecosystem of a free and independent thought process up against a directed ecosystem against that. But with that said—

Senator DAINES. As long as we can keep our freedom, the rule of law, abundant supplies of energy, tax code to incentivized American innovation, I agree with you. The threats, I believe, to our long-term competitiveness are not outside the city but they are right here in this city.

Mr. ESTEVEZ. Let us pass BIA. Let us get CHIPS funding out there.

Senator DAINES. We agree on that. Well, thank you, and I do not want to—we should not be underestimating the threat that China presents long term. I am not betting against the U.S. at all. As long as we stay free, have the rule of law, and have policies that

incentivize innovation, we are going to win. But it is a very real threat.

Mr. ESTEVEZ. I agree with you, Senator.

Senator DAINES. Thank you.

Chairman BROWN. Senator Warner of Virginia is recognized from his office.

Senator WARNER. Thank you, Mr. Chairman, and I appreciate you holding this hearing.

Mr. Estevez, my friend Senator Daines just raised this issue, and I know others have as well. I think it is critically important from a competitiveness standpoint, national security standpoint, that we go ahead and pass the CHIPS legislation. I think almost all of our colleagues understand that we need to have those fabrication facilities built here in America, that, candidly, we are not producing any of the leading edge chips. And as we get below 10 nanometers into even smaller and smaller, to be dependent upon Taiwan is not smart.

I think sometimes we have forgotten, though, that what started this whole debate—and I say this as a former telecom guy—was when we were a little bit asleep at the switch, and China crept up in the 5G domain and managed to set the standards, the rules, the protocols, come forward with a company like Huawei that was extraordinarily important. And I just want to remind my colleagues and I hope you realize, Mr. Estevez, that, you know, in addition to the \$52 billion around CHIPS, there is a billion and a half dollars for investment in the USA Telecom Act that was also included in this legislation that makes sure that we make the investments in not only 5G but the next generation beyond 5G and wireless communications, open radio access network.

Can you talk about what you guys are doing on the BIS tools to make sure that we are looking at beyond 5G technology to make sure that we reclaim some of that leadership we need?

Mr. ESTEVEZ. Thank you for that, Senator. You know, this morning I was listening to NPR, and they used a Wayne Gretzky quote about skating where the puck is going rather than where the puck is. And we need to be doing that, and we are. So it is not just what technologies are there today that need protection. We need to look out and see what is coming down the pike and what should we be thinking about the protections on that. And when I have been talking to companies, that is exactly what I am talking to them about, and it is also what I am talking to my Defense colleagues about.

Senator WARNER. Well, I do think, again, any big or slim CHIPS-related bill, I know everybody has agreed with the USA Telecom piece, that 5G and O-RAN needs to be a part of that, but I appreciate that.

I want to go back again to the CHIPS piece and some of the Huawei entity designation list. I am really concerned, and a number of our—kind of in the memory space, a lot of our domestic manufacturers have complained to me about the Chinese memory manufacturer YMTC. The *Financial Times* just did a major exposé on this that YMTC was providing components, parts to Huawei. You may not be able to talk about all of the specifics of this case, but I have urged the Commerce Department to look very carefully at

YMTC's activities. I think they are typical of a lot of the new Chinese memory and chip-related firms.

How do you make sure we are—whatever you can say about YMTC specifically would be great, but if you can also just generally talk about, you know, how you are investigating potential violations of the Huawei entity list, and how do we make sure we maintain the integrity of our enforcement actions to make sure that these tools have got real teeth?

Mr. ESTEVEZ. Thank you for that. Again, I cannot talk about YMTC in particular or any entity which may or may not be under investigation. However, what we would do, regardless of where the allegation or the information came from, but certainly we would like a multi-sources, including information provided by the intelligence community. We would do a supply chain assessment to see how they are flowing and who they are flowing with, what companies they are doing business with and how that occurred. We would work, again, with not just the BIS enforcement arm but with other agencies. And when we find sufficient data, we would move to put them on the list.

Again, it is all-source data that we need to work on. If we find violations, we will put companies on the list.

Senator WARNER. Well, there are a number of members, I think American companies that raised this concern. I think YMTC deserves that investigation and I believe at the end of the day designation. But I appreciate your answers, sir, and I appreciate the time, Mr. Chairman.

Mr. ESTEVEZ. Thank you.

Chairman BROWN. Thank you, Senator Warner.

Senator Tillis from North Carolina is recognized.

Senator TILLIS. Thank you, Mr. Chairman. Secretary Estevez, thank you for being here. I was happy to support your confirmation.

When I come to this hearing, anytime I talk about export controls, first off, thank you for what you have done for Russia. I think it is having an impact, and the dozens of other nations who have followed suit. But when I look at our greatest threat, it is China. And I look at through three lenses: in the Banking Committee, the venue that we are here today; in my position on Senate Armed Services, where we have received some of the briefings that Senator Toomey has rightfully requested and should receive; and also through the Judiciary Committee.

In the Judiciary Committee in particular, I am Ranking Member on the Intellectual Property Subcommittee, and we have had numerous hearings on China's theft of intellectual property. In fact, down in Charlotte, there is a company called Charlotte Pipe. It has been in the family for almost 100 years. It looks like an old-fashioned foundry. It is high-tech, but its look looks like it was back maybe 75 years ago. You can go to a province in China, and there is a Charlotte Pipe, a complete rip-off of intellectual property. It looks like a Hollywood set of this business in North Carolina, inferior products being shipped and imported into the United States. We have caught them a couple of times, but they just shamelessly do it. And I assume that is with the full approval and agreement with the CCP and Xi Jinping.

If you take a look at their J-20 fifth generation fighter, it looks—in fact, if it were flying out of Cherry Point, I would mistake it as an F-35. Maybe it was just coincidental, or perhaps they stole our intellectual property, and they damn sure did not steal it on the battlefield. They are consistently, as a Government, turning a blind eye toward intellectual property theft. Yeah, they are innovators and they have gotten better, and I agree with Steve Daines, they are an innovator. They have got a middle class that is almost twice the size of our U.S. population. I understand the need for businesses to invest in China. But I also think that we have to match China strategically.

In August, I am going to be on a trip that will take me to South America and Africa, and most of my focus is going to be on Chinese investment in this hemisphere and in Africa that have dual-purpose uses. Virtually every dollar that China invests in outside of their country has a dual purpose, an economic and military purpose, and we have virtually no answer to that.

So in my opinion, we have got to get smart. We have to play the same game that they are playing. And if we do not, then Xi Jinping will achieve his objective of being the economic and military superpower by 2050. And we no longer have to think about the threat of the invasion of Taiwan as hypothetical. We have seen what Putin has done in the Ukraine. It is a real threat. And we only have to look to Hong Kong to see that China would be prepared to do it if they thought they could get away with it.

Think about what would happen if China took Taiwan and how disruptive that would be to the global economy, and particularly the United States economy with the technology that we rely on out of that part of the world.

So I have got a debate club in my office, Senator Toomey. Half of them, if the light shines on them right, it looks just like you in terms of being very careful about controlling outbound investment. The other half, who happens to be the people who sit on the Judiciary Committee, my Judiciary staff, and my Senate Armed Services staff say, “We have got to do something differently here. We have to recognize them differently.” We do have to have free trade with China, but it has got to be fair. And there has to be a consequence when they are not playing by the rules. And they are absolutely not playing by the rules.

And, by the way, on CFIUS, I have had personal experience with CFIUS where I think we have got work to do there. We get some transactions swept up in CFIUS that should not. I think there are some reviews that need to go more quickly. We ended up getting one done that affected a North Carolina-based business. But I do think it is time for us to sit at the table and figure out if we are going to play the same game China is playing or if we are going to let them unilaterally use every device that they have—and we do not. So the only question I have for you in the 30 seconds remaining, when you are taking a look at outbound—or any sort of export controls right now in your lanes—and I know you talk about where the DOD comes in—is the intelligence community and the DOD involved in your decisionmaking process?

Mr. ESTEVEZ. The intelligence community provides information. The DOD is part of the decisionmaking process.

Senator TILLIS. How active are they in the final decisionmaking process? Do they provide inputs, or are they at the table?

Mr. ESTEVEZ. They are at the table.

Senator TILLIS. Good. Last thing here, I ask this of people all the time. What is the best thing in this Congress that could come out that could provide you tools that you think are necessary to match up against the China threat?

Mr. ESTEVEZ. You know, I talked about some resources, you know, certainly some—

Senator TILLIS. So you think you have the authorities, you just need more people?

Mr. ESTEVEZ. There is one authority that is a provision in one of the China bills that would give me authority to do some things on people working with the Chinese intelligence.

Senator TILLIS. Are there any proposals in Congress right now that would not be particularly helpful?

Mr. ESTEVEZ. No—I should not say that, no.

Senator TILLIS. What are they?

Mr. ESTEVEZ. We believe that our interagency process works very well, and that, you know, it needs to remain that way.

Senator TILLIS. OK, so what specific proposals are you concerned with?

Mr. ESTEVEZ. There are proposals around making the first discussion over a licensing decision a public record, so how did the DOD vote? How did DOE vote? How did State vote? And how did Commerce vote? And there is a process that that works, and only 0.14 percent actually gets escalated after discussion, because what we do is we provide information we pull from your question, the intelligence community, and we look at all sources to get the right answers.

Senator TILLIS. Got it. Thank you.

Thank you, Mr. Chair.

Chairman BROWN. Thank you. And, Mr. Under Secretary, follow up a little more on extending authorities that Senator Tillis just raised, what more you need precisely so we understand better.

Mr. ESTEVEZ. Yeah, in ECRA, or maybe it was passed after ECRA, there is a control that supports—stops U.S. persons from supporting Chinese military, and we need it to be a little broader, to Chinese military and the Chinese intelligence community, you know, the surveillance community that are doing things. So it would expand the export control, which I think was the original intent of the legislation. It just came out narrower than it was intended.

Chairman BROWN. OK. Thank you. And, Senator Tillis, thank you for raising that and allowing you to explore a little better.

Your agency, BIS, has done impressive work to build an international coalition that has imposed sweeping export controls in response to Russia's unprovoked war in Ukraine. I spoke in my opening statement about the President's impressive assembling of the coalition in terms of pushing back on Russia and from Sweden, to Switzerland, to Finland, to Germany and beyond. And your export controls have been really important.

How do you evaluate the effectiveness of these controls? How will it inform future actions?

Mr. ESTEVEZ. So we work with, again, our interagency partners and with those countries and certainly with the intelligence community to assess what is going on. And we listen to Russia's own statements. You know, Putin himself made a statement about concerns about the semiconductor—loss of semiconductors coming into Russia. I know from my personal experience, you know, in the Department of Defense you need semiconductors to make a precision guided weapon.

Now, the Russians do not seem to care about precision guided, you know, because they are indiscriminately hitting civilian populations. But the reality is they are going to run out of capability and are going to be incapable of sustaining their force over time.

Chairman BROWN. Thank you. President Biden took office with the campaign promise that "Human rights will be the center of our foreign policy." That, as you know, as the world knows, was a dramatic reversal of his predecessor's foreign policy. What actions has BIS taken to follow through on that promise? And answer also what other actions do you plan to take?

Mr. ESTEVEZ. So human rights are part of the regular license review process, so any license that comes before us, you know, we look to assess whether there is a human rights issue around that. You know, certainly surveillance technology is a great example of that.

We have a number of Chinese firms—I do not have the exact number off the top of my head—that we have put on the entity list related to their use of surveillance technology and also to the suppression of the Uyghur minority in Xinjiang. And, of course, we are working with the interagency on the Human Rights Initiative and what export controls would be appropriate in that vein.

Chairman BROWN. OK. As the President of the Richmond Federal Reserve told me once, "Watch what I do, and let me know that you are watching what I do." And we will be watching you. I understand your good intentions, but we will be watching on human rights, so thank you for that, Mr. Under Secretary.

Last question. You said recently BIS should take the partnerships you build, in responding to Russia, and build a new, your words, "digital export control regime for the 21st century." I am a strong proponent, as a number of people in both parties in this Committee are, of international cooperation and updated efforts that would address civil and military fusion policies, human rights violations, strategic supply chains, and other shared national security and foreign policy concerns.

Describe, if you would, in more detail your work on that effort and discuss, if you would, the conversations with allies on what national security and foreign policy such a regime would address and how you would go about identifying the tools and technology that warrant control.

Mr. ESTEVEZ. Certainly, and when I talk about this, Senator, you know, I am not talking about replacing the existing Missile Control Regime or the Wassenaar Agreement. You know, this is a supplemental. The reality is time has changed since those regimes were put in place. It used to be the U.S., for example, the Department of Defense was the generator of innovative technology. That is not the case. Today it comes from the commercial sector. We have this

great group that we have put together to address the Russia controls, and, again, semiconductors is a great area of that. We have a threat arising from China and from other nations, and we are working with them talking about what would be the appropriate control regime that we should be working together on that. And we are certainly talking to our partners in the EU, the specific nations of the EU, our Five Eyes partners, and our partners in Asia about those issues.

Chairman BROWN. Thank you, Mr. Under Secretary. Let me ask one more question. Senators Menendez and Warren are on the way. One other question. BIS has added a number of parties to the entity list and military end-user list. Describe the end-user tools that BIS uses to address entities of concern. What considerations guide the use of end-user controls?

Mr. ESTEVEZ. So we look at who the exporter says it is going to, and, again, we draw on the full capabilities of the interagency, including the intelligence community, to see who that end user is, who that end user is related to, so we can see if there is diversion potential. And that is how we would make a decision on a licensing agreement or whether someone should go on the entity list.

Chairman BROWN. Thank you. Senator Menendez from New Jersey is recognized.

Senator MENENDEZ. Thank you, Mr. Chairman.

Under Secretary Estevez, we are facing an epidemic of gun violence in our country, and we continue to see armed conflict and even human rights abuses abroad committed with American-made weapons. We are told that export control of semiautomatic weapons are safer at Commerce than at the State Department because BIS has dedicated agents to do end-use monitoring on these firearms after they are exported; whereas, State supposedly does not.

However, isn't it true that such agents are checking to see if such exports are diverted to unapproved persons but not checking for whether or not such firearms are being used for human rights abuses?

Mr. ESTEVEZ. As I just answered Senator Brown before you came in, human rights are part of the licensing review, and certainly for firearms they are at the top of the list for licensing review, and we do that with the Department of State, Department of Defense, and Department of Energy. And when we do our enforcement actions, we would do likewise.

Senator MENENDEZ. But the end-use efforts, isn't it really that they are diverted to—making sure they are not diverted to unapproved persons? You are not really doing human rights monitoring on end use, are you?

Mr. ESTEVEZ. We are doing human rights monitoring in the initial export decision, and should someone use an export inappropriately, we would look at, you know, our other tools, for example, entity list or blocking further licensing.

Senator MENENDEZ. At least at State the Congress was able to review and disapprove such sales above \$1 million on human rights grounds if it so chose. What congressional check has there been since the transfer of jurisdiction on those proposed exports?

Mr. ESTEVEZ. As I believe you are aware, Senator, we have a rule that is going to go into effect on the 18th, on Monday, that will pro-

vide congressional notification regarding weapons over a certain amount, and it precludes our providing to our allies.

Senator MENENDEZ. Yes, I appreciate that, and I was happy to discuss that with Secretary Raimondo. However, even after the rule becomes effective, Congress will not be able to disapprove any such sales. Isn't that correct?

Mr. ESTEVEZ. But you will see them in advance, and you can certainly provide——

Senator MENENDEZ. Let me reiterate my question. Congress will not be able to disapprove such sales. Isn't that correct?

Mr. ESTEVEZ. That is correct.

Senator MENENDEZ. OK. Now, President Biden, when he was a candidate, promised that he would reverse President Trump's transfer of export control of semiautomatic weapons to Commerce and return control to the State Department, which he can do simply by regulation, and in so doing make them subject again to the Arms Export Control Act and, therefore, congressional oversight. Do you know of any progress within the Administration in fulfilling the promise made by the President?

Mr. ESTEVEZ. I do not, Senator.

Senator MENENDEZ. OK. Let me ask you a different question. A New Jersey medical device manufacturer and its union employees received medical grade stainless steel tubing from a longstanding supplier in Korea. The company has applied for and received limited exclusions from the Section 232 quota for this tubing, but managing inventory timing remains a huge and costly challenge even with those exclusions in place. The company has had to estimate its needs far into the future and stockpile tubing for up to a year at a time, costing them about a quarter million dollars annually.

In December 2020, BIS released a list of general approved exclusions for the Section 232 Korea steel quota, and anything classified under the HTS codes on that list are no longer subject to the quota cap. In my constituent company's interaction with BIS, career staff indicated additions to the list would be made over time, but to date, it is my understanding that no new exclusions have been granted under this process.

Can you explain the process and timeline for placing additional HTS codes on the list and what other criteria that are necessary to see additions made to the list?

Mr. ESTEVEZ. On February 22nd, before I was confirmed into the position, BIS put out for public comment asking for comments on additional exclusions to the list. We have received 98 comments to date, and we expect to have a rule out by the end of the year.

Senator MENENDEZ. I hope that BIS can continue to review new applications for general approved exclusions and make new additions where necessary.

One last question. Much of your job involves making sure critical technologies do not fall into the hands of foreign adversaries, human rights abusers, or other rogue actors. Can you explain why maintaining America's technological leadership is so critical to our national security and the mission of BIS?

Mr. ESTEVEZ. Thank you for that, Senator. Having American technology being used to develop military capabilities that are on par with ours certainly threatens our national security. You know,

when I was in the Department of Defense, my job was to arm U.S. forces, to provide the weapons and capabilities that they use, because we never want to put a U.S. soldier, sailor, airman, or marine into a fair fight. And my job right here is to protect American technology from being used by an adversary to do that. That is my North Star, Senator.

Senator MENENDEZ. So, therefore, we want to be in an unfair fight where we are on the side of the unfairness.

Mr. ESTEVEZ. We want to be on—if an adversary is threatening us, we want to win.

Senator MENENDEZ. Right. Thank you very much.

Chairman BROWN. Thank you, Senator Menendez.

Senator Warren from Massachusetts is recognized.

Senator WARREN. Thank you, Mr. Chairman.

I want to ask specifically about military assault weapons like the one that was used on the 4th of July to kill seven people in Highland Park.

Now, Congress should reinstate the assault weapons ban to keep these guns off our streets, but we should not be shipping them to just anyone overseas either. In fact, companies need license from the Federal Government to sell assault weapons overseas. These are called “export licenses.” But in 2020, the Trump administration made it easier to get that permission by putting the Commerce Department in charge instead of the State Department where those permissions had always resided.

This shift is important. The State Department has deep expertise in foreign instability, human rights abuses, and terrorism. The Commerce Department specializes in promoting U.S. industry overseas, even the gun industry. In the 2020 campaign, President Biden promised to reverse the Trump decision and put export control back with the State Department, but as of today that has not happened.

So, Under Secretary Estevez, how many billions of dollars in assault weapons sales has Commerce approved since it took over export control in March 2020?

Mr. ESTEVEZ. I will have to get back to you on the exact amount, Senator, so I will get you that—

Senator WARREN. Do you want to do an estimate? I think your records show—

Mr. ESTEVEZ. I think the website shows \$15 billion.

Senator WARREN. \$15.7 billion.

Mr. ESTEVEZ. Across all types of weapons, not just assault weapons.

Senator WARREN. So Commerce approved \$15.7 billion in weapons sales in its first 16 months on the job, and by comparison, when the State Department was making these decisions, it approved \$12 billion on average in the same time period, including some weapons that never got transferred to Commerce. So if you do the math, that is about a 30-percent increase.

Now, that is a huge boon to the gun industry. The \$15.7 billion in Commerce-approved exports is nearly as large as the current size of the entire \$19 billion U.S. gun manufacturing industry.

Export control law gives Commerce a lot of authority to disapprove license requests, including if such weapons sales threaten our national security or undermine our foreign policy.

So, Under Secretary Estevez, how often since March 2020 has the Commerce Department actually denied the gun industry's request to export these assault weapons?

Mr. ESTEVEZ. Senator, a couple of things, and it is a small percentage, and, again, I do not have the percentage off the top of my head.

Senator WARREN. Well——

Mr. ESTEVEZ. But can I answer a couple other points? The State Department is part of my review process. The State Department can stop a sale.

Senator WARREN. I am asking, now that you have the approval process, what have you done? How many have you disapproved in that time period? Do you know the number?

Mr. ESTEVEZ. I do not know the number, Senator.

Senator WARREN. It is four-tenths of 1 percent. That is, less than one-half of 1 percent of the applications are disapproved, which sounds a lot like the Commerce Department is rubber-stamping these license applications, including to places like Mexico, where corruption puts these weapons in the hands of criminals, or the Philippines, where there are multiple reports of security forces shooting civilians.

Now, President Biden has stated clearly that he supports cracking down on assault weapons both at home and overseas, so let me ask, Under Secretary Estevez: Can you explain how increasing assault weapons export licenses by 30 percent and turning down less than one-half of 1 percent of applications is consistent with the President's stated objectives? Is the Commerce Department working for the President or working for the gun industry here?

Mr. ESTEVEZ. Senator, that also includes sales to people like Ukraine that are using those weapons against the Russians right now.

Senator WARREN. I have no doubt.

Mr. ESTEVEZ. So this is an interagency process now that it has moved to Commerce. There is the power of the Department of State that brings State's jurisdiction to that discussion, the Department of Defense, and the Department of Energy. So it is——

Senator WARREN. So wait a minute——

Mr. ESTEVEZ. —an interagency process that approves gun licenses.

Senator WARREN. Excuse me, Under Secretary——

Mr. ESTEVEZ. It is not just the Commerce Department.

Senator WARREN. Excuse me. What happened is authority was transferred to the Commerce Department, and what has happened is that it has a minuscule disapproval rate and the weapons sales have gone up dramatically.

Look, the Commerce Department is helping put more assault weapons in more hands, and this needs to stop. It is time to put overseas gun sales back in the hands of the State Department where someone can exercise better judgment over it.

Thank you, Mr. Chairman.

Chairman BROWN. Thank you, Senator Warren.

Senator Moran is on his way back. Senator Toomey has one more question.

Mr. ESTEVEZ. Certainly.

Senator TOOMEY. Mr. Estevez, we spoke briefly earlier about how to determine whether or not U.S. technology is involved in the development of China's stealth bomber and hypersonic missile, and we talked about a briefing, and you agreed that you would do the briefing. But subsequent dialog suggested that it might be useful to involve the DNI in that briefing. Will you work with us to make sure that we get a comprehensive insight into this and the input of the DNI?

Mr. ESTEVEZ. I absolutely will work with you on that, Senator.

Senator TOOMEY. Thank you very much.

Chairman BROWN. Thank you, Mr. Under Secretary. It looks like Senators Moran and Van Hollen we thought were on the way but they may not be. Thank you for the work that BIS is doing on many fronts to impose economic consequences against Russia in the wake of their invasion of Ukraine. Your work is so important. Thanks for the use of tools at your disposal to defend our national security.

For Senators who wish to submit questions for the hearing record, those questions are due 1 week from today, Thursday, July 21st—my wife's birthday, I might add. Under Secretary Estevez, please submit your responses to questions for the record within 45 days from the date you receive them.

The Committee on Banking, Housing, and Urban Affairs is adjourned.

[Whereupon, at 11:10 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN SHERROD BROWN

Today we welcome our witness, Alan Estevez, who serves as Under Secretary for Industry and Security at the Department of Commerce.

I thank Ranking Member Toomey and his staff for their help in confirming Under Secretary Estevez and the two Assistant Secretaries at the Bureau of Industry and Security—Thea Kendler for Export Administration and Matt Axelrod for Export Enforcement.

This is the first time since we passed the Export Control Reform Act in 2018 that Congress has fully confirmed BIS leadership.

Because of this Committee's work, for the first time since 2013 we have a full, confirmed Federal Reserve Board.

Yesterday we confirmed a fourth member of the Ex-Im board. We finally have a fully functioning Export-Import bank.

And for the first time in our history, these nominees are beginning to look more like America.

The world changed this year on February 24, when Russia invaded Ukraine, continuing its barbaric war on the Ukrainian people and their sovereignty.

Putin has been shocked by two things:

The strength of the Ukrainian resistance and the skill of this President in assembling and uniting a broad coalition, the likes of which we haven't seen in decades—Germany, Finland, Switzerland.

We've isolated Russia and limited its ability to access the tools and technologies it needs to continue its grotesque war against Ukraine.

And BIS has been integral in our international response to siphon off Russia's access to military material. It quickly rolled out a sweeping series of rules designed to stall and degrade Russia's military and technological capabilities.

BIS targeted Russia's defense, aerospace, and maritime sectors, and it applied controls to U.S. exports and to items produced abroad that use U.S. software, technology, or equipment.

Since February 24, BIS issued 12 new rules, ramped up enforcement activity, and continued to build what Assistant Secretary Axelrod called "the broadest expansion of multilateral export controls among like-minded partners since the creation of CoCom back in 1949.

The results have been impressive.

Exports to Russia by countries who have imposed sanctions have fallen by 60 percent.

At the same time BIS weakened Russia's military, it committed to ensuring that those items that benefit the Russian people, like medical supplies, are still available.

This ability to distinguish bad actors—whether they're State or non-State actors—while still allowing innocent civilians to benefit from U.S. exports is crucial, as the agency builds on this new international coalition to address other national security and foreign policy challenges.

To that end, Under Secretary Estevez, I am encouraged by your statements calling for strengthening or supplementing our existing multilateral regimes.

Enhancing our multilateral regimes requires patience—by BIS and Congress. And we must work with allies to identify the items and technologies that present a risk to our collective national security.

This is important work, and I am pleased to hear that it is one of Under Secretary Estevez's top priorities.

Back in 2018, when this Committee worked to enact the Export Control Reform Act, we included policy statements, guiding BIS in developing export control policy.

One of those guiding principles is that our national security requires that the United States maintain our leadership in science, technology, engineering, and manufacturing.

That value should guide our export control policy. And it should also guide our work in Congress.

We do not want to be at the mercy of our competitors—or our adversaries—for technology and other inputs vital to a 21st century economy. Dependency on countries like China poses a huge economic risk and an unacceptable national security risk.

It's why we need investments in research and development, and in our fellow citizens.

We have an innovation and competition bill in conference that would do just that.

Ranking Member Toomey and his staff have worked in good faith with me and my staff to negotiate this Committee's conference provisions. I thank them for that important work.

We have reached bipartisan agreements on provisions with the House Foreign Affairs Committee and the House Financial Services Committee.

It is time for us to vote on and pass a final bill that promotes U.S. science, technology, and manufacturing, so that we can maintain U.S. economic leadership.

This bill will create thousands of good-paying jobs in Ohio and around the country—jobs in growing industries, jobs where you can build careers. In my State, more than 10,000 jobs are at stake. Business leaders and labor leaders are both desperate for this investment.

The head of the Ohio Chamber of Commerce—former Republican Congressman Steve Stivers—and the head of the Ohio Business Roundtable—former Republican Congressman Pat Tiberi—have been particularly vocal about this support.

We must act now.

For decades, at the behest of corporate America, policymakers of both parties have passed bad tax policy and bad trade policy that allowed these companies to move American jobs and supply chains and technology abroad—always in search of lower and lower wages.

And when the production moves abroad, the innovation moves with it.

We invented semiconductor chips. Now 90 percent of chips are made overseas.

We have to fix that. Now.

Americans have waited long enough. We should pass this bill this month.

If Congress is serious about the threats that face us, it must be similarly serious about supporting American innovation.

PREPARED STATEMENT OF SENATOR PATRICK J. TOOMEY

Thank you, Mr. Chairman. Under Secretary Estevez, welcome.

The Bureau of Industry and Security, or BIS, determines which U.S. goods are too sensitive to be shipped abroad. In the face of China's drive for dominance in key tech sectors, BIS's mission today is as important as ever.

By setting U.S. export control policy on items used for both civilian and military purposes, BIS effectively has the power to reshape the supply chains of entire industries. That means BIS must craft export controls in a prudent, thoughtful, and effective manner that advances U.S. national security interests without unduly harming America's economic interests.

The issue I would like to focus on today is a legislative concept that has received a growing amount of attention in recent months, falls squarely in the jurisdiction of this Committee, and would unquestionably impact BIS's mission and workflow, if enacted. I am referring to a concept known as "outbound CFIUS."

The idea is to establish a new agency within the Executive branch, and give this agency vast, potentially unchecked authority to regulate, intervene in, and block all kinds of potential activities, including prohibiting Americans and U.S. firms from investing in, selling to, or buying from companies in certain countries, most notably China.

Outbound CFIUS could also provide the President with extremely broad authority to determine which industries to subject to regulation. It is not just semiconductor firms that would be affected. Any industry determined to be in the national security interest of the United States could be impacted.

President Biden's recent invocation of the Defense Production Act for baby formula is just the latest reminder of how the Executive branch can abuse the term "national security." President Trump also abused the notion of "national security," having the Commerce Department laughably assert in a 232 investigation that the import of foreign cars was a threat to our national security.

In fact, it appears that Mr. Estevez agrees with this, because during his confirmation hearing before this Committee he said to me, "232 is an important tool . . . Section 232 needs to be looked at in a hard national security lens, Senator. It shouldn't be used willy-nilly." I share Mr. Estevez's concern about national security authorities being abused by a President "willy-nilly."

It is not an overstatement to suggest that hundreds of thousands of U.S. companies and tens, if not hundreds, of billions of dollars in commerce could be impacted by outbound CFIUS.

The rise of China presents the United States with the greatest security challenge we've faced since the end of the Cold War. I am clear eyed about the fact that the Chinese Communist Party has embarked on a concerted, whole-of-Government campaign to surpass the technological leadership of the United States in areas that will underpin geopolitical military and economic power for decades to come. But how we address this challenge matters.

Doing outbound CFIUS, and getting it wrong, could impede the national security agencies—such as BIS or CFIUS—that are already doing important work on China. Getting it wrong could also severely harm the United States.

We cannot prevail in this contest with China by emulating China, like the China competition bills before the Senate envision. Instead, we must out innovate China and protect our intellectual property from theft and illicit transfer.

That means ensuring that the United States remains the single greatest global destination for capital formation, research and development projects, and the smartest minds in the world to come and work. Getting outbound CFIUS wrong puts all this into jeopardy by disincentivizing the flow of capital, ideas, and people to come to the United States.

There are many important questions about outbound CFIUS that remain unanswered. For example, what is the problem outbound CFIUS is attempting to solve? How do current laws and authorities, such as export controls, address or fall short of addressing this problem? How would outbound CFIUS affect the United States as a destination for capital formation and technological innovation?

I am not the only one concerned about the reasoning and implications of standing up an outbound CFIUS mechanism. I have here a letter from three former officials from the last Administration who directly oversaw CFIUS and export controls.

It raises concerns about the scope and justification for outbound CFIUS, and it calls for any such mechanism to be grounded in a clear statutory law brought about through regular order. If Mr. Estevez's predecessors are concerned about the way in which outbound CFIUS is playing out, I think he should be too.

In addition, 11 trade associations representing hundreds of thousands of companies and workers sent a letter to Congress expressing opposition to the inclusion of outbound CFIUS in the China competition bills under consideration. I ask that these two letters be entered into the record of this hearing.

Given these concerns, Congress must take the time to properly evaluate the outbound CFIUS concept rather than rushing to enact it.

PREPARED STATEMENT OF ALAN F. ESTEVEZ

UNDER SECRETARY FOR INDUSTRY AND SECURITY, U.S. DEPARTMENT OF COMMERCE

JULY 14, 2022

Chairman Brown, Ranking Member Toomey, Members of the Committee, thank you for inviting me to testify today on the work of the Commerce Department's Bureau of Industry and Security, or BIS.

BIS's mission is to advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership.

We execute this mission by imposing appropriate controls on exports and reexports of lower capability military items, dual-use items (i.e., those items having both commercial and military or proliferation applications), and predominantly commercial items. We have the authority to seek criminal and administrative sanctions when appropriate for violations of our export controls. We also play an important role in Commerce's analysis and support of our industrial base, and the Department's participation on the Committee on Foreign Investment in the United States (CFIUS).

Put another way, our primary goal is to prevent malign actors from obtaining or diverting items, including technologies, for unauthorized purposes, in order to protect our national security and advance our foreign policy objectives while supporting the competitiveness of our key industries.

BIS's mission has never been more relevant. We face ongoing national security threats from Nation States—China, Russia, Iran, North Korea—as well as from terrorists and other non-State actors. However, on top of the traditional threats posed by those actors, we also must contend with an evolving threat landscape and the use of commercially available technologies to further activities of concern, including human rights abuses.

As Under Secretary of Commerce for Industry and Security, I view my role as the "Chief Technology Protection Officer" of the United States. BIS operates at the nexus of national security and technology, and export controls are a unique and powerful tool for responding to the modern threat environment that we face. This is particularly true when we work together with our allies and partners.

We are in an important moment for our national security, and today I will focus on BIS's role administering and enforcing export controls to address four critical challenges: first, our response to Russia's further invasion of Ukraine; second, the

pace threat that China represents; third, the identification of emerging and foundational technologies essential to national security; and finally, the need to build a durable, multilateral technology security framework for the future use of export controls.

Responding to Russia's Further Invasion of Ukraine

BIS has robust authorities under the Export Control Reform Act of 2018, or ECRA. Using those authorities, BIS has imposed sweeping export controls on Russia for its unjustified, unprovoked, and premeditated further invasion of Ukraine, and on Belarus for its substantial enabling of that invasion. And thanks to the additional resources Congress provided to BIS in the Ukraine Fiscal Year (FY) 2022 supplemental spending bill, we are prepared to sustain and expand those actions against Russia and Belarus.

Our goal is to choke off exports of technologies and other items that support Russia's defense industrial base, including defense, aerospace, and maritime sectors, and to degrade Russia's military capabilities and ability to project power. While the impact of our export controls will only increase over time as Russia is unable to repair, replace, and replenish its military hardware, we are seeing substantial impacts of our actions in the data available to date:

- Since the start of the invasion on February 24 through July 1, 2022, U.S. exports to Russia in categories of items subject to new U.S. export license requirements decreased by 95.9 percent by value as compared to the same period in 2021.
- Overall U.S. exports to Russia have decreased by approximately 88 percent by value over the same period in 2021 (February 24–July 1, 2021).
- Analysis of trade data conducted by the Peterson Institute for International Economics (PIIE) shows that, of the 54 countries that make up approximately 90 percent of Russia's imports, those with similar export controls against Russia in place have seen total exports to Russia decline by a cumulative 60 percent since the invasion. Exports to Russia from countries that have not imposed similar controls are also down 40 percent.
- PIIE goes on to point out that “the inaccessibility of foreign tech and components is hitting Russia's maintenance; supply; and future development of chips, guided missiles, tanks, cars, planes, and much more. Russia's own economy ministry is projecting a GDP contraction of up to 12.4 percent in 2022.”

There are numerous open-source reports on the need for Western semiconductors as key inputs to Russian weapons systems. Since our controls have fully taken effect, there has been a 74 percent reduction by value of global exports of semiconductors to Russia compared to the same period in 2021 (March–May). This has prompted Putin himself to issue public concerns about where Russia will source these critical inputs.

We have also taken multiple actions that have impacted Russia's aerospace sector, which is reliant on U.S. and European manufactured planes, parts, and service necessary to maintain them. There have been reports that Russia will have to ground between half and two-thirds of its commercial fleet by 2025 in order to cannibalize them for parts due to the export controls and enforcement actions we have implemented. And as our recent Entity List actions demonstrate, where we identify companies that attempt to backfill our restrictions, we will take swift action.

These are just some examples of the impact our controls are having to date. This is one of the most aggressive and robust uses of export controls against another country, and these impacts would not be possible without the unprecedented level of coordination with our allies and partners around the world.

While there is an appropriate role for unilateral export controls, as Congress noted in ECRA, “[e]xport controls that are multilateral are most effective[.]” If other countries supply the same types of items that the United States restricts, the U.S. controls will be ineffective for two reasons. First, the countries or parties of concern will still acquire the items at issue. Second, U.S. technology leadership will be threatened if foreign competitors can undercut U.S. companies and earn revenue to invest in research and development. Thus, coordinating with allies and partners also helps keep a level playing field for U.S. companies and helps maintain U.S. technology leadership and competitiveness, all of which contribute to national security, as described in ECRA.

Thanks to the hard work done by the Biden administration—from the President on down—we have built a coalition of 37 other countries so far who have agreed to adopt substantially similar controls on Russia and on Belarus.

Our message to countries that have not joined our restrictions on exports to Russia is that if they share our horror at Russia's aggression against Ukraine and our respect for the rule of law, they should join the United States and our partner countries around the Indo-Pacific and Europe in imposing stringent restrictions on exports to Russia.

To maximize the effectiveness of our controls, we have conducted extensive outreach to the public to educate them on the changes. BIS conducts regular outreach to the exporting community to inform and share best practices, and utilizes international partnerships to educate foreign companies about U.S. export controls. Since February 24, we have conducted outreach on the new controls to over 3,000 entities and individuals.

In addition, we are aggressively enforcing the new controls. We deploy a variety of resources and tools to ensure effective enforcement, including leveraging relationships with other law enforcement agencies, the Intelligence Community, and international partners. BIS conducts physical inspections (e.g., end-use checks and port inspections/detentions) to detect illicit procurements, and we investigate potential violations of U.S. export controls and, if appropriate, vigorously pursue criminal and civil penalties. Since Russia's further invasion of Ukraine on February 24, we have detained or seized 218 shipments valued at \$90 million.

Related to my earlier statements about Russia's deteriorating commercial aviation industry, we have tracked and publicly released a list of over 150 aircraft that we believe operated in violation of our Russia and Belarus controls, in order to provide notice to the world that servicing these aircraft is itself violative of our rules. We also recently issued our first public charging letter against Russian oligarch Roman Abramovich related to his improper export of two private planes, alongside a seizure warrant for the planes obtained by the Department of Justice. We have issued nine temporary denial orders, or TDOs, against various Russian airlines, which effectively cut off not only their right to export items subject to our regulations from the United States, but also their right to receive or otherwise participate in exports from the U.S. of such items.

The Pacing Challenge: China

As we continue our robust response to Russia's further invasion of Ukraine, we remain focused on aggressively and appropriately using our tools to contend with the long-term strategic competition with the People's Republic of China (PRC).

The PRC threat to our national security and foreign policy interests is real. My north star at BIS as it relates to China is to ensure we are appropriately doing everything within our power to prevent sensitive technologies with military applications from getting into the hands of China's military, intelligence, and security services.

Export controls are at the forefront of the many tools that the Biden administration is using to coordinate and respond to China's destabilizing activities. We are using our controls to address China's military-civil fusion strategy that seeks to divert dual-use technologies to military uses, military modernization, WMD program development, human rights abuses, and efforts to destabilize the Indo-Pacific region. Confronting these actions protects our national security and advances our values and interests, as well as those of our allies and partners. This is a dynamic threat environment, and we are constantly evaluating our existing authorities and thinking about how we can employ our tools to maximum effect.

We continue to maintain comprehensive controls related to the PRC, including requiring a license for: all military and spacecraft items under our jurisdiction; all multilaterally controlled dual-use items; a large number of dual-use items with extensive commercial applications if the item is intended, entirely or in part, for a military end use or military end user in the PRC; and all items under our jurisdiction, if the item is exported knowing it will be used in certain WMD programs or if it is intended, entirely or in part, for military-intelligence end uses or end users in China. In addition, the Export Administration Regulations (EAR) prohibit certain U.S. person activities that would support WMD-related activities or military-intelligence end use or end users in China absent authorization. Thus, the EAR's licensing requirements for China seek to prevent activities that threaten U.S. national security and foreign policy interests while allowing commercial activities that do not raise such issues.

We also use our Entity List to identify parties of concern, many of whom are subject to license requirements for all items under our jurisdiction, regardless of the sensitivity of the item. Currently, we have nearly 600 Chinese parties on our Entity List—107 of those added during the Biden administration. These parties have been added for a variety of reasons ranging from supporting China's military modernization and WMD programs, to supporting Iran's WMD and military programs, to fa-

cilitating human rights abuses in Xinjiang. These parties include those involved in artificial intelligence, surveillance, biotechnology, and quantum computing.

We are continually assessing available open-source, proprietary, and classified information, in coordination with our interagency partners, for the addition of other parties to the Entity List and other restricted party lists maintained by BIS in connection with the enabling of China's military-civil fusion strategy and other malign activities.

Addition to the Entity List means that anyone seeking to export or transfer items under Commerce jurisdiction to a listed party must first seek a license to do so from Commerce. As with all license applications, those applications are generally reviewed by the Departments of Commerce, State, Defense, and Energy. As a general matter, such license applications for parties on the Entity List are reviewed under a presumption of denial. For those entities not subject to a comprehensive presumption of denial, the Entity List provides clear policies on the types of items and transactions that may be approved on a case-by-case basis. Thus, companies are likely to only submit license applications for proposed transactions that may be approved by the interagency process.

In the select instances where there is disagreement among the agencies on whether to approve the license, there is an established process for any agency to initiate further escalation and review. During FY 2021, only 0.14 percent of all applications submitted were appealed to the Assistant Secretary level. While the agencies may have different perspectives on individual cases, we all bring helpful expertise to the process and can reach accommodation on almost all applications. And when we cannot, the interagency review and escalation process forces us to bring our best arguments to the table to help shape U.S. export control policy.

In addition to the Entity List, we also maintain the Unverified List, which includes parties for which we cannot verify their bona fides (i.e., legitimacy and reliability relating to the end use and end user of items subject to the EAR). Earlier this year, we added 33 Chinese parties to the Unverified List as BIS was unable to verify their bona fides because an end-use check could not be completed satisfactorily for reasons outside the U.S. Government's control. Because of this designation, no license exceptions can be used to export to these parties, and BIS is imposing a pre-license check for any license application involving these parties.

We know that the PRC is determined to advance its military capabilities by illicitly acquiring U.S. technology. Our enforcement team at BIS is dedicated to preventing this from happening by utilizing all of our criminal and administrative investigative tools, as well as regulatory actions like the Entity List and Unverified List, to aggressively enforce our export control rules. For example, 21 percent of the Office of Export Enforcement's current investigations involve China as the ultimate destination. And in FY 2021, 66 percent of criminal penalties and 40 percent of administrative penalties levied related to export violations involving China, totaling almost \$6 million, as well as resulting in 226 months of incarceration. In addition to monetary penalties, we also have a powerful administrative tool to deny export privileges. For example, in June, we imposed a temporary denial order on three interrelated companies—Quicksilver Manufacturing Inc., Rapid Cut LLC, and U.S. Prototype Inc.—that contracted with U.S. defense and aerospace customers to 3-D print items based off sensitive prototype space and defense technologies. The three companies illegally sent the blueprints and technical drawings to China to create 3-D prints, which were then shipped back to the United States. BIS's action prevents these three companies from participating in, or benefiting from, any export transaction while our investigation continues.

China remains a complex challenge in the competition between democracies and autocracies. We continue to assess the effectiveness of our controls to address our national security and foreign policy concerns related to the PRC and analyze whether the current threat landscape requires new action. We are closely reviewing our approach to China, seeking to maximize the effectiveness of our controls.

Identifying Emerging and Foundational Technologies Essential to National Security

One such assessment is our continuous review to identify emerging and foundational technologies essential to the national security of the United States, as required under Section 1758 of ECRA. As many of you know, this topic has attracted considerable attention, and for very good reason. BIS works closely with our interagency colleagues to stay informed on new technologies with national security implications and determine whether we need to recalibrate controls on new or existing technologies subject to our jurisdiction. Since enactment of ECRA, BIS has established 38 new controls on emerging technologies, including controls related to semiconductor production, biotechnology, and quantum computing. All but one of

these controls are multilateral, with the one unilateral control pending multilateral agreement.

As part of interagency groups led by the National Security Council, we have finished reviewing seven technology groups, which has contributed to proposing and finalizing new controls. In many cases, these reviews have also found that our current controls were sufficient to capture emerging technology roadmaps. Where updates were needed, we have prioritized updating and adding new controls. In addition, BIS has identified technologies that were also identified through CFIUS filings to propose potential controls on emerging and foundational technologies.

We're also continuing to do more to involve parts of the Government that are closer to the development and funding of new technologies. I am working with the Department of Defense Under Secretaries for Acquisition and Sustainment and for Research and Engineering to establish a critical technologies review board. This board will help BIS to understand the technologies DoD is investing in for military use, and help us provide the appropriate controls for those technologies.

We are also working to propose or implement new controls faster and more efficiently. As part of a May 23, 2022, rule, we informed the public that we would no longer characterize new controls as corresponding to "emerging" technology or corresponding to "foundational" technology, instead referring to the technologies at issue as "Section 1758 technologies." As we noted in that rule, this approach reflects the difficulties in drawing meaningful and functional distinctions between technologies for purposes of fulfilling our statutory obligations under Section 1758 of ECRA. Attempting to do so, without statutory definitions for those terms, resulted in delays in proposing and implementing new controls on such items because there is no clear, consistent agreement within the Government and in the public on how to apply the terms "emerging" and "foundational" to specific technologies.

Attempting to characterize a technology as either "emerging" or "foundational" reduces our flexibility to respond to real-time developments in rapidly changing technological landscapes. For example, the marine toxins identified in our most recent proposed rule defy common attempts to define "emerging" and "foundational" as these toxins are naturally occurring items that are not new and have never been on the Commerce Control List. Calling such items "Section 1758 Technologies" maximizes our flexibility and effectiveness. As Under Secretary for Industry and Security, my fundamental principle is that if there is a technology that could potentially harm our national security (and is essential to our national security), we want to assess it and if appropriate, impose controls on it—regardless of whether it can be labeled "emerging" or "foundational."

While we will use the term "Section 1758 Technologies" going forward, we will continue to review whether additional controls are warranted for technologies that may be viewed as "foundational," or "emerging." We are statutorily required to do this. We are also statutorily required to consider three criteria when identifying emerging or foundational technologies: (i) the development of emerging and foundational technologies in foreign countries; (ii) the effect export controls may have on the development of such technologies in the United States; and (iii) the effectiveness of export controls on limiting the proliferation of emerging and foundational technologies to foreign countries. Thus, imposing new, unilateral controls on a technology that foreign suppliers can backfill or that a target country already has would be ineffective and primarily undermine U.S. development of such technologies. That is the key challenge with more mature technologies and raises the importance of obtaining multilateral or plurilateral controls for such items.

Multilateral Cooperation Essential to Our Security

That brings me to the final topic I want to discuss today: furthering multilateral cooperation to more timely address national security and foreign policy concerns.

Given the great work we have done with our partners with regards to Russia, and given the threats posed by China—and other malicious actors in the world—I believe we have been presented with a great opportunity to further coordinate with our allies.

In all the export control policy areas I have described, it is clear that cooperation with allies and partner countries is essential to the effectiveness of these controls. To that end, we are involved in working with various groups, including the European Union in the Trade and Technology Council's Export Control Working Group and Japan in the Japan-United States Commercial and Industrial Partnership. We are also leading an export control effort in the Indo-Pacific Economic Framework for Prosperity.

Additionally, we are working with colleagues across the interagency to lead the multilateral Export Controls and Human Rights Initiative, which we announced during the Summit for Democracy. Through this effort, we are working with foreign

Government partners to establish a voluntary, written code of conduct around which like-minded States could pledge to use export control tools to prevent the proliferation of software and other technologies used to enable serious human rights abuses.

We continue to monitor the effectiveness of the current multilateral regimes and, when necessary, identify areas of plurilateral cooperation in certain technologies with other supplier countries. All four multilateral regimes maintain key controls in restricting the proliferation of conventional arms, dual-use items, and items related to WMD activities. In addition, to mitigate today's threats, we must also work with like-minded Governments of supplier countries of certain technologies of concern, including to identify ways to use export controls to limit the use of technologies to commit human rights abuses.

Finally, enforcement is critical to ensuring effective export controls and we are working with partners across the globe on this effort as well. We recently announced an enhanced export enforcement partnership with Canada, and we are working with the European Commission and its Member States on a similar coordination effort. Our Export Control Officers around the globe are also working with enforcement partners in countries stretching from Europe to East Asia, including Singapore and the United Arab Emirates, to enhance export control enforcement and prevent the diversion of U.S.-origin items.

Ultimately, for the United States to maintain effective export controls and technology leadership, which itself is a part of our national security, we need to work in cooperation with others. Our work with the 37 other countries to implement the Russia controls helps provide a blueprint for advancing further. We have momentum on export controls that I will be working to carry forward as we build a new technology security architecture.

We have a lot of work ahead of us on all of these fronts, and there are many more areas where BIS is doing important work that I have not discussed. I am proud to be serving in this critical moment, and I value the partnership and collaboration with you and your staffs as we tackle these challenges together.

Thank you again for the honor of inviting me here to testify today, and I look forward to your questions.

**RESPONSES TO WRITTEN QUESTIONS OF CHAIRMAN BROWN
FROM ALAN F. ESTEVEZ**

Q.1. During the hearing on July 14, and at the House Foreign Affairs Committee's hearing on July 19, members asked questions regarding the recent transfer of certain munitions from the U.S. Munitions List to the Commerce Control List. Though this transfer of items occurred prior to your service at BIS, please describe any changes to existing controls, licensing policies, or enforcement authorities that resulted from the transfer. Please also describe the process for reviewing license applications related to these items, including consideration given to potential end uses and end users, and any trends related to license applications for these items.

A.1. Under prior Administrations, defense articles on the U.S. Munitions List (USML) in the International Traffic in Arms Regulations (ITAR) were transferred from the export control jurisdiction of the Department of State to the Department of Commerce if such items did not provide the United States with a critical military or intelligence advantage or, in the case of weapons, have an inherently military function, for export control purposes. Within this process, the Department of State and Department of Commerce published final rules on January 23, 2020, effective March 9, 2020, that revised USML Categories I (firearms, close assault weapons and combat shotguns), II (guns and armament), and III (ammunition/ordnance) and transferred items that no longer warranted export control on the USML in the ITAR to the Commerce Control List (CCL).

Following these changes, the Department of Commerce's Bureau of Industry and Security (BIS) regulates exports of non-fully automatic firearms up to .50 caliber (12.7mm) inclusive, which includes semi-automatic, bolt-action, lever-action, pump-action, single-shot and double rifles, pistols, and revolver type firearms, ammunition, and related items, which are subject to a worldwide license requirement by BIS for export from the United States. BIS imposed additional restrictions on these items when they transferred to Commerce jurisdiction, such as restricting the use of license exceptions and imposing restrictive license review policies on certain end users, such as narcotics traffickers. Also, for those licenses approved, the amount that may be exported is also limited by the applicable import license/certificate restrictions of the importing country. Since the transfer of jurisdiction, BIS has further tightened restrictions, such as to address the concerns over technology or software for 3D printing of firearms.

License applications for firearms exports under Commerce jurisdiction are reviewed by Commerce, Defense and State to address, among other things, human rights, and impacts to regional stability with the potential exports. Assessments by BIS Licensing Officers, as well as the other agencies that review these license applications, are updated on a continuous basis to respond to changes in specific countries, as well as additional information that is received on the bona fides of the parties identified in license applications, including , from the Watch List administered by the Department of State's Directorate of Defense Trade Controls, diplomatic and other reporting. Thus, the same agencies that reviewed license

applications for these items when they were on the USML continue to do so today.

In addition to these front-end restrictions, BIS has Export Enforcement agents—Federal law enforcement officers—whose mission is to ensure that firearms exports are not diverted to activities that violate U.S. law or would otherwise be contrary to our national security or foreign policy interests. And BIS makes arrests and works with our Justice Department partners to seek indictments when appropriate. The addition of BIS enforcement resources builds upon those previously available when these items were on the USML in the ITAR.

Importantly, there are many approvals for licenses of firearms exports to Government entities of allies and partners, such as Ukraine in its defense of its sovereignty and territorial integrity against Russian aggression, and it is in our national security and foreign policy interests to support the Ukrainian people. The largest by dollar value for firearms exports under the Export Administration Regulations (EAR) is Canada. For example, for calendar year 2021, BIS approved 278 firearms licenses valued at \$347.6 million and 130 ammunition licenses valued at \$595.7 million. The amount of firearms approved is based on a 4-year projection in many instances, so the total number of actual firearms exported is lower. BIS continually assesses its licensing policies, but always reviews export license applications consistent with U.S. national security and foreign policy interests.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN
FROM ALAN F. ESTEVEZ**

Q.1. President Biden supports the reinstitution of a domestic assault weapons ban, which would prohibit the manufacture, sale, transfer, and importation of assault weapons and high-capacity ammunition in the United States. If such a ban were enacted, which of the 17 Export Control Classification Numbers (ECCNs) that were created to control items moved from the United States Munitions List (USML) Categories I–III to the Commerce Control List (CCL) would be considered assault weapons and high-capacity ammunition and therefore subject to the ban?

A.1. BIS interprets this question to refer to firearms described in H.R. 1808, “Assault Weapons Ban of 2022”, and BIS believes this would apply to a subset of firearms described in ECCN 0A501. Such firearms are currently subject to a worldwide license requirement by BIS for export from the United States. BIS also imposed additional restrictions on these items when they transferred to Commerce jurisdiction, such as restricting the use of license exceptions and imposing restrictive license review policies on certain end users, such as narcotics traffickers, and also has worked to address the concerns over technology or software for 3D printing of firearms.

License applications for firearms exports under Commerce jurisdiction are reviewed by Commerce, Defense and State to address, among other things, human rights, and impacts to regional stability with the potential exports. Assessments by BIS Licensing Officers, as well as the other agencies that review these license applications, are updated on a continuous basis to respond to changes

in specific countries, as well as additional information that is received on the bona fides of the parties identified in license applications, including from the Watch List administered by the Department of State's Directorate of Defense Trade Controls, diplomatic and other reporting. Thus, the same agencies that reviewed license applications for these items when they were on the USML continue to do so today.

In addition to these front-end restrictions, BIS has Export Enforcement agents—federal law enforcement officers—whose mission is to ensure that firearms exports are not diverted to activities that violate U.S. law or would otherwise be contrary to our national security or foreign policy interests. And BIS makes arrests and works with our Justice Department partners to seek indictments when appropriate. The addition of BIS enforcement resources builds upon those previously available when these items were on the USML.

Q.2. When you appeared before the Committee on July 14, we discussed aggregate data on the Commerce Department's approval of export licenses for assault weapons and some other items, and you committed to providing me with the exact dollar value of approved export licenses for semiautomatic, or assault, weapons since the

Commerce Department gained jurisdiction over these exports in March 2020. Since March 2020, how many licenses for the export of assault weapons and high-capacity ammunition (as defined under Question 1) has the Commerce Department approved? What is the dollar value of the export licenses for assault weapons and high-capacity ammunition that Commerce has approved since March 2020? What is Commerce's approval rate on export license applications for assault weapons and high-capacity ammunition since March 2020?

A.2. On January 23, 2020, the Department of Commerce, Bureau of Industry and Security (BIS) published a final rule, effective March 9, 2020, in conjunction with a Department of State final rule to revise Categories I (firearms, close assault weapons, and combat shotguns), II (guns and armaments), and III (ammunition/ordnance) of the United States Munitions List (USML) and transfer items that no longer warrant export control on the USML in the International Traffic in Arms Regulations (ITAR) to the Commerce Control List (CCL) (85 FR 4136, Jan. 23, 2020). Since this transfer of jurisdiction, through August 1, 2022, BIS has approved 13,867 applications valued at \$10.06 billion dollars' worth of firearms, parts, and components described in ECCN 0A501. The approval rate is over 98 percent, the value of firearms and components denied was over 38 million dollars. Note that ECCN 0A501 includes far more than just semiautomatic firearms of which "assault weapons" as defined in the referenced act would be a subset of these. Note also that these applications are valid for 4 years and in many instances involve projected sales which may be lower than what is ever physically exported.

License applications for firearms exports under Commerce jurisdiction are reviewed by Commerce, Defense and State to address, among other things, human rights, and impacts to regional stability with the potential exports. Assessments by BIS Licensing Officers, as well as the other agencies that review these license appli-

cations, are updated on a continuous basis to respond to changes in specific countries, as well as additional information that is received on the bona fides of the parties identified in license applications, including from the Watch List administered by the Department of State's Directorate of Defense Trade Controls, diplomatic and other reporting. Thus, the same agencies that reviewed license applications for these items when they were on the USML continue to do so today.

Q.3. We also discussed concerns about the export of American-made assault weapons to countries like Mexico, where corruption puts these weapons in the hands of criminals, and the Philippines, where reports have emerged of security forces carrying out extrajudicial killings against civilians. To which countries, and in what quantities (dollar value and license number), has Commerce approved exports of assault weapons (as defined under Question 1) since March 2020? To which countries, and in what quantities (dollar value and license number), have these weapons actually been exported since March 2020?

A.3. On January 23, 2020, the Department of Commerce, Bureau of Industry and Security (BIS) published a final rule, effective March 9, 2020, in conjunction with a Department of State final rule to revise Categories I (firearms, close assault weapons, and combat shotguns), II (guns and armaments), and III (ammunition/ordnance) of the United States Munitions List (USML) and transfer items that no longer warrant export control on the USML in the International Traffic in Arms Regulations (ITAR) to the Commerce Control List (CCL) (85 FR 4136, Jan. 23, 2020). BIS applications in general would not differentiate between those types of firearms considered "assault weapons" in this legislation and other types of firearms in the same caliber range because multiple types of firearms are all included within ECCN 0A501. In calendar year 2021 for Mexico there were 1,744 firearms shipped to Mexico, of these 790 were pistols and revolvers and 954 were rifles of all types and calibers of which "assault rifles" could possibly be a subset of the 954. For the Philippines, in calendar year 2021 there were 15,797 firearms shipped to the Philippines of these 15,130 were revolvers and pistols and 667 were rifles of all types and calibers of which "assault rifles" could possibly be a subset of the 667.

With respect to exports to Mexico, BIS also notes its administration of the United States' commitment to the Organization of American States (OAS) Model Regulations for the Control of the International Movement of Firearms, their Parts and Components and Munitions (OAS Model Regulations), which were developed to assist OAS member countries to implement the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials (Firearms Convention). Pursuant to this, BIS requires licenses for the export of specified firearms to OAS member countries and requires the submission of an import certificate from the recipient countries' Government prior to the issuance of any such license.

Q.4. For each country listed in the answer to Question 4, what percentage of exports went to Government agencies? What percentage of exports went to nongovernment entities and individuals?

A.4. For Mexico, all license applications for these items are for export to the Government of Mexico, which then supplies the items to specific parties. With respect to the Philippines, BIS would have to do a manual review of all approved licenses to determine the percentage that went to nongovernment entities and individuals. All parties in license applications are reviewed by Commerce, State, and Defense, including to review for human rights concerns, regional stability concerns, or potential risk of diversion to other parties of national security or foreign policy concern.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR TILLIS
FROM ALAN F. ESTEVEZ**

Q.1. As you know, State-subsidized drone companies based in China control over 90 percent of the U.S. and global markets and have put many U.S. companies out of business. The largest of those, DJI, is on the Entity list and Chinese Military Industrial Complex Company (CMIC) list for supporting human rights abuses and genocide in China. The Department of Defense and some civilian agencies have also banned the use of DJI, and other drones made by PRC companies, due to well-known national security and cybersecurity concerns. And many in Congress are working to ban their use governmentwide.

Do you agree with your predecessor's decisions to place DJI on the Entity and CMIC List, and that they are a threat to national security?

A.1. It is a matter of public record that DJI was added to the Entity List in December 2020 by the Commerce Department, Bureau of Industry and Security (BIS), after the usual interagency review by the End-User Review Committee (ERC) made up of representatives of the Departments of Commerce, State, Energy, and Defense, and, where appropriate, the Treasury, because the company "enabled wide-scale human rights abuses within the People's Republic of China through abusive genetic collection and analysis or high-technology surveillance, and/or facilitated the export of items by the PRC that aid repressive regimes around the world, contrary to U.S. foreign policy interests," as BIS stated in its December 18, 2020, rule. The effect of DJI's addition to the Entity List is that the export, reexport, or in-country transfer of any item subject to the Export Administration Regulations (EAR) to DJI requires a license from the Commerce Department. DJI remains on the Entity List. DJI remains on the Entity List, and I have no reason to second guess its placement on the Entity List.

Q.2. Will you commit to this Committee that you will advocate that DJI stays on the Entity List?

A.2. BIS commits to continually monitoring parties on the Entity List for activities that are contrary to the national security and foreign policy interests of the United States. Under the Export Administration Regulations (EAR), parties on the Entity List may request Commerce to be removed. Removal from the Entity List requires unanimous agreement of the End-User Review Committee (ERC), made up of representatives of the Commerce Department (Chair), Departments of Commerce, State, Energy, and Defense, and, where appropriate, the Treasury. DJI remains on the Entity

List, and I have no reason to second guess its placement on the Entity List. Consistent with Executive Order (EO) 13918, it is the policy of the United States to prevent to use of taxpayer dollars to procure UAS that prevent unacceptable risks and are manufactured by, or contain software or critical components from, foreign adversaries and to encourage the use of domestically produced unmanned aerial systems (UAS).

Q.3. What other authorities available to BIS can you consider to protect the homeland from the threats posed by DJI and other drones made by PRC companies?

A.3. BIS is continually assessing technologies, end uses, and end users in developing appropriate export controls to protect U.S. national security and foreign policy interests. BIS possesses a variety of tools beyond the Entity List, such as further restricting the licensing policy applicable to exports under the Export Administration Regulations (EAR) to countries or parties and transmitting “Is Informed” letters (i.e., letters to individual companies informing them of additional license requirements related to specific parties and/or items). When appropriate, these additional license requirements can be imposed because of end-use or end-user concerns.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD
LETTER SUBMITTED BY THE BUREAU OF INDUSTRY AND SECURITY

July 14, 2021

The Honorable Sherrod Brown
Chairman
Committee on Banking, Housing, and Urban Affairs
U.S. Senate
534 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Pat Toomey
Ranking Member
Committee on Banking, Housing, and Urban Affairs
U.S. Senate
534 Dirksen Senate Office Building
Washington, DC 20510

Chairman Brown and Ranking Member Toomey:

We respectfully request that the following statement be submitted for the record of the Senate Committee on Banking, Housing, and Urban Affairs oversight hearing on U.S. export control policy. This hearing is a timely opportunity to register our concerns about an “outbound” investment screening proposal known as the Committee on National Critical Capabilities (CNCC). Several legislative drafts creating the CNCC have been released publicly, including the original standalone bill S.5049, and our comments here pertain to all of them. While intended to address in particular, the growing threat of China, the legislation’s expansive approach across multiple government agencies and leading sectors of the U.S. economy instead is likely to cause considerable confusion and potential economic disruption at a time when the U.S. economy is strained by inflation and geopolitical turmoil – a situation that China and other adversaries will be able to exploit.

As former senior national security officials who oversaw export controls and the Committee on Foreign Investment in the United States (CFIUS) at the Departments of Commerce and Treasury, and the White House, we believe that China’s military and economic rise poses the greatest long-term challenge to the security of our nation and those nations around the world who share America’s values. For these reasons, we were proud to have worked with the Banking Committee through its deliberative process to achieve the passage and implementation of the Export Controls Reform Act (ECRA) and the Foreign Investment Risk Review and Modernization Act (FIRRMA)—long-overdue revisions to U.S. export control and foreign direct investment authorities to address these technology security concerns.

The effectiveness of these two laws is rooted in three factors in particular – specificity, authority, and accountability.

- *Specificity* refers to the need for precisely tailored government authorities. National security measures must be limited, fact-based, clear, and targeted in order to both be effective and foster compliance. Effective enforcement is only possible when regulations are well-understood within the government and the private sector.

- *Authority* refers to the need to ensure that any new government power is situated where it can be most effectively exercised, is not duplicative of or in conflict with other authorities and is subject to vigorous congressional oversight.
- *Accountability* refers to ensuring that the U.S. government has both sufficient long-term resources and appropriate mechanisms—finely tuned and targeted as well—to enforce implementing regulations and ensure their compliance.

FIRMA and ECRA clearly meet these tests. It is not at all clear to us that the CNCC does. As currently conceived, its overly broad and unspecified mandate leaves far too much authority subject to the interpretation and implementation by varied agencies in the Executive branch, now and in the future.

It is critical that these concerns and any others be fully addressed before any new program or authorities are created. Matters of a complex nature, especially those dealing with three highly challenging areas—technology, financial markets, and national security—are best considered through a process that enables adequate opportunity for thorough consideration by both policymakers and the public who would be subject to such new and far-reaching authorities. Policy makers need to understand the potential impacts of this legislation on government agencies and on the U.S. economy. Rushing through expansive legislation without an understanding of likely impacts and potential unintended consequences poses considerable risks that could advantage our adversaries. In short, “regular order” should be applied to Congress’ consideration of this important issue. Since your committee has clear jurisdiction of this type of authority—both in terms of export controls and capital flows—we hope that you will consider convening hearings on this matter. Finally, we believe that any such screening mechanism should be firmly grounded in a new and explicit authorizing statute, as opposed to relying on Executive orders or other broad authorities such as the International Emergency Economic Powers Act. Again, speaking as former senior officials who were responsible for the stewardship of similar authorities, the ultimate objective of government policy has the potential to be hindered in the absence of clear, accountable, and enforceable measures.

We understand and share the motivation in Congress to meet the challenge posed by the Chinese Communist Party and its policies and strategic goals. Taking steps without adequate consideration and deliberation, however, could be severely detrimental to the very national security interests we all seek to preserve. Thank you for consideration of our views.

Sincerely,

Thomas P. Feddo
Former Assistant Secretary for Investment Security, Department of Treasury

Mira Ricardel
Former Deputy National Security Advisor, Executive Office of the President
Former Under Secretary for Industry and Security, Department of Commerce

Richard Ashooh
Former Assistant Secretary for Export Administration, Department of Commerce