HEARING ON U.S.-CHINA RELATIONS IN 2021: EMERGING RISKS

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

THURSDAY, SEPTEMBER 8, 2021

Printed for use of the
United States-China Economic and Security Review Commission
Available via the World Wide Web: www.uscc.gov

UNITED STATES-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2021

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

CAROLYN BARTHOLOMEW, *CHAIRMAN*
ROBIN CLEVELAND, *VICE CHAIRMAN*

Commissioners:

BOB BOROCHOFF
JEFFREY FIEDLER
KIMBERLY GLAS
HON. CARTE P. GOODWIN
ROY D. KAMPHAUSEN
DEREK SCISSORS
HON. JAMES M. TALENT
MICHAEL R. WESSEL
ALEX N. WONG

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106–398 (codified at 22 U.S.C. § 7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107–67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109–108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (Dec. 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter and statutory mandate are available online at: https://www.uscc.gov/charter.

CONTENTS

THURSDAY, SEPTEMBER 8, 2021

HEARING ON U.S.- CHINA RELATIONS IN 2021: EMERGING RISKS

Panel I: Beijing's Assertion of "Comprehensive Jurisdiction" Over Hong Kong

Panel II: The CCP's Control of Markets and Data

Administration Panel: Administration Views on U.S. Export Controls

Panel III: Assessing Export Controls and Foreign Investment Review

QUESTION FOR THE RECORD

U.S.-CHINA RELATIONS IN 2021: EMERGING RISKS

THURSDAY, SEPTEMBER 8, 2021

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, D.C.

The Commission met in Room 430 of Dirksen Senate Office Building, Washington, DC and via videoconference at 9:30 a.m., Vice Chairman Robin Cleveland and Commissioner Kimberly Glas (Hearing Co-Chairs) presiding.

OPENING STATEMENT OF VICE CHAIRMAN ROBIN CLEVELAND HEARING CO-CHAIR

VICE CHAIRMAN CLEVELAND: Good morning to everybody and welcome to our final hearing of 2021. In recent years, we've concluded our hearing cycle to take a look back at the year and consider anything that was not originally addressed by other hearings.

At the same time, this hearing is a valuable opportunity for us to preview the year ahead. I'm glad that eight of our 11 witnesses today are new to the Commission, which is always helpful, helpful to us in generating fresh ideas and broadening our perspective.

As we try to anticipate the next year in U.S.- China relations, that view is very much overshadowed by increasingly aggressive tactics the CCP has employed to assert greater control over both its companies and to the detriment of U.S. investors, as well as Chinese growth and their economy.

What happened to the Ant Group in November 2020 was the harbinger of a Chinese regulatory backlash against non-state companies. The party insists that data security and disorderly expansion of capital motivate its assault on Chinese corporations like Ant, Didi, and Tencent.

But, in fact, these judgments are unclear and unpredictable and throw company valuations into unstable swings, leaving investors, and companies, and countries to wonder who the CCP will target next.

The indiscriminate regulatory pressure is not just a problem for billionaires in the world. Many U.S. investors have tied fortunes to the growth of U.S. listed Chinese companies, investments that we have known always have been steeped in risk.

Over the last several months, this risk has become clearer and far larger than previously understood. Rather than comply with U.S. law, the Chinese government is wresting its companies away from the oversight of U.S. regulators and directing them back to Shanghai, Shenzhen, and Hong Kong.

Not only do U.S. investors stand to lose billions from Chinese companies disappearing or underselling their way out of U.S. exchanges, they likely have little legal recourse.

Our witnesses will help illustrate the scope of this problem and offer insight on the CCP

strategy. Today we will consider China's efforts to abuse not only U.S. funds but technology.

As our name indicates, we have a clear mandate to understand the intersection of both economic and national security. These areas are deeply intertwined in the design of the U.S. export control and foreign investment screening systems. The design and continual improvement of these systems is crucial to protecting key strategic technologies from misappropriation.

We're pleased later to hear from the Department of Commerce Bureau of Industry and Security, followed by a set of expert practitioners who will help us understand the legal and regulatory structure that might be refined to address threats from China. I'm going to turn to my Co Chair Kim Glas who will talk a little bit about what your panel is going to present.

And today, just for the understanding of members, we will proceed alphabetically for the first panel starting with Carolyn B. And on the next panel, do reverse alphabetical. So, to my co-chair Kim, welcome, first co-chairing! Glad you're here. And please proceed.

PREPARED STATEMENT OF VICE CHAIRMAN ROBIN CLEVELAND
HEARING CO-CHAIR

Hearing on "U.S.-China Relations in 2021: Emerging Risks"

Opening Statement of Commissioner Robin Cleveland

September 8, 2021

Washington, DC

Welcome to our final hearing of 2021. In recent years, we have concluded our hearing cycle to take a look back at the year to recover anything not originally addressed by our other hearing agendas. At the same time, this hearing is a valuable opportunity for us to preview the year ahead. I am glad that eight of our 11 witnesses today are new to the Commission, which is always helpful for us in generating fresh ideas and broadening our perspective.

As we try to anticipate the next year in U.S.-China relations, that view is overshadowed by increasingly aggressive tactics that the Chinese government has employed to assert greater control over its companies, to the detriment of U.S. investors as well as their own growth. What happened to Ant Group in November 2020 was just the beginning of a Chinese regulatory backlash against prominent nonstate companies that are supposedly deviating from the Party's wishes and direct control. The Party insists that data security and the "disorderly expansion of capital" motivate its attacks on Chinese corporations like Didi and Tencent. In fact, these judgments are opaque and seemingly arbitrary, throwing company valuations into unstable swings and leaving investors and companies alike to wonder who the CCP will target next.

The CCP's indiscriminate regulatory pressure is not just a problem for the Jack Ma's of the world. Many U.S. investors have tied fortunes to the growth of U.S.-listed Chinese companies, investment that have always been steeped in risk. Over the last several months, this risk has become clearer and far larger than previously understood. The Chinese government is wresting its companies away from the oversight of U.S. regulators to direct them back to Shanghai, Shenzhen, and Hong Kong. Not only do U.S investors stand to lose billions from Chinese companies disappearing or underselling their way out of U.S. exchanges, they likely have little to no legal recourse. Our witnesses will help illustrate the scope of this problem, the CCP's strategy, and protections for U.S. investors.

Today, we will consider China's efforts to abuse not only U.S. funds, but also U.S. technology. As our name indicates, we have a clear mandate to understand the intersection of both economic and national security. These areas are deeply intertwined in the design of the U.S. export control and foreign investment screening systems. The design and continual improvement of these systems is crucial to protecting key strategic technologies from misappropriation. We are be

pleased to hear from the Department of Commerce's Bureau of Industry and Security today, followed by an experienced set of practitioners, to understand how these tools can continue to be refined as threats from China evolve.

OPENING STATEMENT OF COMMISSIONER KIMBERLY T. GLAS
HEARING CO-CHAIR

COMMISSIONER GLAS: Thank you, Vice Chairwoman Cleveland. I want to thank all our witnesses for appearing before us today. And appreciate all their excellent testimonies and look forward to engaging in this important discussion. I also want to extend our sincere appreciation to the Commission staff for their outstanding work preparing for this hearing.

This hearing is intended to examine the challenges over the past year and new complexities that have emerged. We will hear from expert witnesses about those challenges and relay context on what the U.S. Congress and other decision makers should be doing in response.

2020 was like a year like no other and our witnesses are going to speak to that today. The Chinese government has pursued ruthless aggressive campaign to bring Hong Kong to its heels, demonstrating a total disregard for its commitments to the international community and to the people of Hong Kong.

This has taken many forms starting with passing a sweeping National Security Law last year that undermines free and open society and makes fundamental changes to Hong Kong's judicial procedures and legal systems that will have a profound impact for generations to come. And one of the most concerning developments this past year, the Hong Kong government changed election rules to ensure that no advocates of democracy will ever be able to run for office, let alone get elected to the legislature. From intimidating and incarcerating activists, to shutting down unions critical to the government's policies, to firing educators, and to silencing media groups, any of these actions are alarming. The magnitude combined is what is profound. The question is for our witnesses is how the U.S. government can act even more swiftly based on these disturbing developments, and what the implications are, if we don't.

Another focus of the hearing today is on export controls. It has emerged in recent years as a powerful tool to protect U.S. national security, as well as prevent the transfer of technology that can be used to perpetuate human rights abuses in places like Hong Kong and China. Congress passed landmark legislation, but is our application of that legislation and our ability to respond swiftly, keeping pace with the dynamic global environment?

Given the rapid evolution of cutting-edge technology, this makes this issue even more complex. China's methods of obtaining critical U.S. technologies has become more elaborate in globalized supply chains.

We need to evaluate the strengths and the weaknesses of our system to ensure that emerging threats that pose questions. To what extent are we responding quickly? And are we utilizing all the tools at our disposal? And to what extent do we need more tools?

I look forward to hearing from all of you. And before we begin today, I'd like to remind you that the testimonies and transcript from today's hearing will be posted on our website, uscsc.gov.

This is the Commission's final hearing for 2021 and we will resume our hearing cycle in January of 2022. And with that, Robin, I will turn it back to you.

PREPARED STATEMENT OF COMMISSIONER KIMBERLY T. GLAS
HEARING CO-CHAIR

Hearing on "U.S.-China Relations in 2021: Emerging Risks"

Opening Statement of Commissioner Kim Glas

September 8, 2021

Washington, DC

Thank you, Vice-Chairman Cleveland, and good morning. We are grateful to our witnesses for their excellent prepared testimony and look forward to an engaging discussion on these important matters.

Like 2020, this year was uniquely challenging in many ways. The Chinese government continued its ruthless campaign to bring Hong Kong to heel, demonstrating a total disregard for its commitments to the international community and the people of Hong Kong. Since Beijing implemented the sweeping National Security Law last year, Hong Kong's formerly free and open society has become unrecognizable.

In January, the Hong Kong government arrested dozens of the city's most prominent democracy advocates, kicking off a campaign of intimidation and incarceration that strikes at the heart of Hong Kong's society. Democratic organizations and community groups in Hong Kong, many of which were pillars of the community for years, have been forced to disband as their organizers have been arrested and imprisoned.

In one of the most concerning developments this year, the Hong Kong government changed election rules to ensure that no advocates of democracy will be able to even run for office, let alone get elected to the legislature. This new policy seems to snuff out any hope of Hong Kongers reclaiming the rights that have been stolen from them.

Hong Kong's information space is now in many ways eerily similar to that of the Mainland, as authorities have slowly but surely silenced independent media groups, shut down unions critical of the government's policies, and fired educators. The U.S. government has acted swiftly to respond to these disturbing developments by removing some special treatment of Hong Kong, though I look forward to hearing from our witnesses about additional policy tools to address the city's loss of freedoms.

Export controls have emerged in recent years as a powerful tool to protect U.S. national security as well as to prevent the transfer of technology that can be used to perpetuate human rights abuses in places such as Hong Kong and China. In 2018, Congress passed landmark bipartisan

legislation with the Export Control Reform Act and the Foreign Investment Risk Review Modernization Act, paving the way to addressing threats from Chinese industrial policies and predatory investment. These tools are crucial to strengthening U.S. economic growth and protecting national security.

Of course, these efforts must be balanced with maintaining U.S. technological competitiveness and an open investment environment. The challenge is not insurmountable, but the rapid evolution of cutting-edge technology does make it more complex. As China's methods of obtaining critical U.S. technologies become more elaborate across heavily globalized supply chains, we also recognize the need to monitor and re-evaluate the strengths and weaknesses of our systems to deal with new and emerging threats.

All of these topics require serious and careful consideration. I look forward to learning from all of you, and I especially look forward to your recommendations.

Before we begin, I would like to remind you that the testimonies and transcript from today's hearing will be posted on our website, www.uscc.gov. This is the Commission's final hearing for 2021, but we will resume our hearing cycle in January 2022.

PANEL I INTRODUCTION BY VICE CHAIRMAN ROBIN CLEVELAND HEARING CO-CHAIR

VICE CHAIRMAN CLEVELAND: Thank you. Carolyn, given your involvement in Hong Kong, is there anything you want to say at this point, or wait until questions?

CHAIRMAN BARTHOLOMEW: I'll go ahead and wait until questions.

VICE CHAIRMAN CLEVELAND: Okay.

CHAIRMAN BARTHOLOMEW: Thank you for noticing.

VICE CHAIRMAN CLEVELAND: Yes, you have been a fierce, formidable and long-standing advocate for democracy. So all right, to our panelists actually, I'm going to say something just for one quick moment because otherwise I'll forget. This is also Alex's last hearing. Is that right?

ALEXANDER BOWE: Yes.

VICE CHAIRMAN CLEVELAND: So I want to thank you for all you've done for the Commission and for putting this hearing together, in particular. Alex is going to be leaving us and going on to even more exciting adventures where putting hearings together are not a part of the problem.

So on the first panel, the panel will examine what the Chinese government calls its exercise of "comprehensive jurisdiction" over Hong Kong. Our first witness will be Michael Davis, Global Fellow at the Woodrow Wilson International Center for scholars. Mr. Davis was a professor in the law faculty at the University of Hong Kong until late 2016, long a public intellectual in Hong Kong. I've just read your recent book. His scholarship engages a range of issues relating to human rights, the rule of law and constitutionalism in emerging states. The Hong Kong Foreign Correspondents Club awarded him a 2014 human rights press award for his commentary in the South China Morning Post on the 2014 Hong Kong Umbrella Movement. Congratulations. Mr. Davis, thank you for being with us here today.

Next, we'll hear from Angeli Datt, Senior Research Analyst for China, Hong Kong and Taiwan at Freedom House. Ms. Datt works on the China Media Bulletin and monthly bilingual digest providing news and analysis on media freedom developments related to China and a project on Beijing's global media influence. Prior to joining Freedom House, Angeli was the Deputy Director of Research at Chinese Human Rights Defenders and wrote under the pen name Frances Eve. Welcome, Ms. Datt.

Our third expert on this panel will be Samuel Chu, Founder and former Managing Director of the Hong Kong Democracy Council. The Washington D.C. based nonpartisan voice for Hong Kong's pro-democracy movement and Hong Kongers in the U.S.
Hong Kong authorities issued arrest warrants against Samuel in 2020, making him the first foreign citizen to be targeted under the National Security Law. Samuel, we really appreciate you making the trip from the West Coast and welcome your testimony.

Finally, we will welcome, I think online, is that right? Yes, there you are. Maureen Thorson, partner with Wiley Rein. Her practice focuses on U.S. customs law and international trade litigation. She's a licensed customs broker and has particular expertise in classification and country of origin analyses and has advised multiple clients with respect to duties on Chinese origin goods. Ms. Thorson also specializes in anti-dumping and countervailing duty litigation before the U.S. Court of International Trade and the U.S. Court of Appeals for the Federal Circuit. Thank you for testifying today, Ms. Thorson.

So I'd like to remind witnesses that there are a lot of us. We ask a lot of questions. Keep your opening statements, brief, to seven minutes so that we can pepper you with lots of questions.

With that, Mr. Davis, please begin. And to remind, we'll start with Carolyn and proceed in alphabetical order on questioning. Mr. Davis?

OPENING STATEMENT OF MICHAEL C. DAVIS, GLOBAL FELLOW, WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

MR. DAVIS: Thank you, Madam Chair, and thank you for the Commission to invite me. My experience is mostly on the ground in Hong Kong. And as the head, the Chair said, it's a frontline experience in the democracy movement now for 30 years. And so, I've kind of watched all of this unfold. But when I look at what's happened in the last year, my jaw drops. You can't make this up. I mean, when we watch what happened in Afghanistan, and we worry about the Taliban --I mean, in some ways, China is not bringing a religious extremism, but it's bringing our kind of form of government extremism to an open society. And literally, they've checked all the boxes. And I think what they've come up with, in this global debate on democracy versus authoritarianism, I think for Hong Kong, they come up with a model of what the authoritarian version looks like. They're not going to, when people say China might impose the Chinese model on places, they're not really talking about the CCP, or some version of it taking over and countries, but societies that have soft authoritarianism, or moderately open societies, how to provide more controls.

And this is a textbook case. We all know what Hong Kong looked like before this all happened. Even up until a couple years ago, the kind of intervention, as I outlined in written statement I submitted today, was softer, it was more influence peddling, interference from the central government. But that all really changed dramatically in 2019. So, when I look at the model, as a constitutional lawyer, I can say that Hong Kong, the guarantees and promises to Hong Kong were remarkable. The Sino British Joint Declaration was indeed something that a lot of us had hoped for. And it promised all the good stuff, human rights, the common law would be maintained, and so on. But it had some holes in it as well.

But two things I think are really important to the recent debate that it promised was that mainland laws would not apply in Hong Kong, except under Annex III. A few of them would be added, if they involved things beyond Hong Kong's autonomy. And the other was that Mainland officials would not interfere in local operations. All of this has gone out the window, now.

Now, I think there were two fundamental problems in the original agreement. One was that Beijing retained the absolute power to interpret the basic law. And this has plagued Hong Kong from day one. And the other has been foot dragging over democracy. Hong Kong people in their wisdom long understood that this government they have now, that's largely appointed by Beijing, would not defend Hong Kong's autonomy, and therefore its rule of law. And in fact, it has not. And so, the demand for democracy, which was promised in the Basic Law, is, for that reason, the wisdom of understanding that they needed a government not to go to war with China, but simply to have a voice to express the concerns and guard the core values of Hong Kong people. So I think this is what was on the table.

The NSL comes along. It's remarkable how everything is there. One is they rammed it through without even consulting Hong Kong society. Another is the NSL, the National Security Law, is superior even to the Basic Law. And the Court of Final Appeal made that clear, in the case involving Jimmy Lai's bail. In fact, what they said is the rule on bail there was an exception to the common law rule. In effect, any human rights violations in the NSL are exceptions because the Court said we do not have the power to exercise constitutional review over this. They do that over all the other laws in Hong Kong. Hong Kong has long had, like America, constitutional review. The NPC also can override the courts in interpreting that law. And they didn't trust judges. So they were very clear. Let's have a select list of judges that can interpret

the law locally. So this was another thing that I think really grates in Hong Kong because opinion polls show Hong Kong people's core values, among them, the rule of law is at the top. And the independence and finality of the courts is at the top.

Well, the courts aren't just suffering from that law. They're suffering from pressure from Beijing officials, from mainland media, from Beijing supporters in Hong Kong, literally attack the judges if they don't give the right ruling in these cases. And so the National Security Law says that if judges make statements that violate the National Security Law, then they will be dismissed from this list. And how would they make statements? The common law tradition in Hong Kong, these judges aren't politicians. They stay in the courthouse. The only statements are going to make are in court. In other words, if you don't rule the way we want, we'll take you off the list. And so this is another thing.

They set up two organizations to implement this. And neither one of them is subject to judicial review. There's a committee, and there's a so-called office for safeguarding national security, just beyond the reach of the courts. But the crimes themselves are vague and they apply all over the world. So if you committed here, if we today commit succession, subversion, terrorism, or collusion with foreign forces, then we could be in violation of the law, as Samuel found out sitting in this country. There's been 150 arrests already. These are remarkable arrests. The one that struck me most recently was the first arrest. That was Tong Ying kit. He actually is the only case I know that has some kind of violence involved because he was running a motorcycle through police cordons. Almost all the other cases involve speech. They're crimes of speech, only. But his case involved that. And he had a slogan that said, revolution, liberate was revolution of our time, liberate Hong Kong revolution of our times.

And they had to decide whether this was inciting independence. And the entire decision did not mention human rights once. Even though, some people said, well, the NSL says human rights are preserved in Article 4. In that judgment, that the court did not mention that there's an international human rights standard in a free speech case for incitement. That there must be intent, imminent, unlawful action and it must be likely to occur. It did not mention it. So it didn't come up at all. So I understand from friends who know lawyers that the lawyers tried to raise it, but it was just dismissed out of hand. Of course, the most notorious case, Jimmy Lai, I think everyone's familiar with Jimmy Lai. So, I won't go into that. But they've shut down his newspaper, a very strong signal to free speech.

The warrant for Samuel, sitting here, these things are all notorious. The attacks on judges for granting bail or for dismissing cases and I think this goes beyond the National Security Law, to all these public order laws that already existed. This kind of attitude of aggressive enforcement, is comprehensive. So Martin Lee, who's known to people here, as well, was convicted in a public order case. And the sedition crime, they argued, the one under the common, under the British system that hadn't been used since 1970, is --they're using the NSL to enforce it, in effect, applying NSL rules.

So all of this is to say to people don't participate in democracy. And then, that that wasn't enough. Of course, they have passed the new election reforms, which as the Chair said, essentially, bar everybody, anybody from participating in the democratic process. You do so at your peril.

There's a whole line of committees and even the police that will investigate you. So these are the kinds of things I outlined in my statement. Like I said, you couldn't make this up. This is real. Thank you.

PREPARED STATEMENT OF MICHAEL C. DAVIS, GLOBAL FELLOW, WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

September 8, 2021
Professor Michael C. Davis
Global Fellow, Woodrow Wilson International Center; Professor of Law and International Affairs, Jindal Global University; and a former Professor of Law, University of Hong Kong
Testimony before the US-China Economic and Security Review Commission
Hearing on "US China Relations in 2021: Emerging Risks"

Background

The situation in Hong Kong before the recent crackdown is well known to this Commission and the world. Hong Kong has long been viewed as a global city at or near the top of global rankings for basic freedoms and the rule of law. It has been a widely admired city with a distinct brand of local culture lodged between East and West, a global financial center on par with other great centers of finance and trade, and at the same time a hub of the arts and culture that has long captured the world's imagination, all very much secured by a vigorous civil society, human rights and the rule of law.

In the 1984 Sino-British Joint Declaration,[1] China guaranteed under its "one country, two systems" formula, that Hong Kong's way of life would be preserved for fifty years from the 1997 handover, along with its core values of human rights and the rule of law. This was all to be included in a Basic Law, which was ultimately promulgated in 1990.[2]

The Basic Law provides for the promised high degree of autonomy, human rights, and the rule of law, as well as the "ultimate aim" of "universal suffrage." With limited exception, related to matters outside the scope of autonomy,[3] mainland laws were not to apply, and mainland officials were not to "interfere in affairs which the Hong Kong Special Administrative Region administers on its own in accordance with this law." [4] Conditioned on these commitments, foreign governments, including the US, recognized Hong Kong as a distinct entity for purposes of trade and other exchanges. Critical weaknesses that would prove the undoing of the model included Beijing control over the interpretation of the Basic Law, with the courts in a subordinate role,[5] and Beijing's foot-dragging over the promised democratic reform to achieve universal suffrage.

[1] Constitutional and Mainland Affairs Bureau (Hong Kong), "Joint Declaration of the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the People's Republic of China on the Question of Hong Kong," (hereinafter "Joint Declaration") December 19, 1984, https://www.cmab.gov.hk/en/issues/jd2.htm . Although Chinese officials often say the Joint Declaration was fulfilled upon the handover, Article 7 binds both governments to fulfill all of its provisions extending for fifty years.
[2] The Basic Law of the Hong Kong Special Administrative Region (hereinafter, "Basic Law") https://www.basiclaw.gov.hk/en/basiclaw/index.html
[3] Basic Law, Article 18 allows for some mainland laws outside the scope of autonomy to be added to Annex III.
[4] Basic Law, Articles 22.
[5] Basic Law, Article 158 assigns the power of interpretation to the National People's Congress Standing Committee (NPCSC), with local courts allowed to interpret it in adjudicating cases. While courts review local legislation, they are not allowed to review national legislation and are bound by NPCSC rulings. *Lau Kong Yung v. Director of Immigration*, FACV Nos. 10 and 11 of 1999 (Hong Kong Court of Final Appeal, December 3, 1999),

In spite of these weaknesses, Kong Kong's rule of law and its status as an open society remained largely intact in the first few years after the handover. Hong Kong often secured the top spot in the Heritage Foundation's Index of Economic Freedom and saw its rule of law ranked among the top in the world.[6] The draining away of autonomy and associated guarantees was mostly a matter of growing Beijing interference long before the hardline takeover we are seeing today.[7]

The undemocratic government subservient to Beijing proved not to be adept at guarding Hong Kong's autonomy. The first blatant warning signs came in 2003 when the Hong Kong government proposed the so-called Article 23 legislation. Article 23 of the Basic Law required Hong Kong "on its own" to enact certain national security legislation. When the Beijing appointed Chief Executive and his cabinet put forth draft legislation, which posed several risks to basic freedoms, alarm bells rang. A half-million protesters took to the streets to demand retraction of the bill, as would ultimately be done when one of the government's supporters, the Liberal Party, bulked and withdrew its support from the bill.

Growing public awareness that Hong Kong's capacity to guard its autonomy would depend on the promised democratic reform, led to equally large protests for democracy in 2004. This demand would become a constant theme in Hong Kong politics, in the 2012 protests against the government's proposed patriotic education, in the 2014 "umbrella movement" protesting government foot-dragging over the promised democratic reform, and in the 2019 protests against the government's proposed extradition bill. The flawed extradition bill aimed to jump over the long-stalled negotiations with the mainland over an extradition arrangement and would have allowed people to be extradited to the mainland without sufficient human rights protections. When the bill was withdrawn the protest again morphed into protests for democratic reform.

As evident in the continuing protests demands for Basic Law compliance, Hong Kong protesters have not sought a local government constantly at odds with Beijing, but they have clearly hoped for a government that would find its voice to guard autonomy and protect the city's core values. Long ignoring popular demands to fulfill Basic Law commitments, the Beijing and Hong Kong governments only have themselves to blame for the growing opposition. The 2020 National Security Law[8] (NSL), imposed directly by Beijing, represents a refusal to take responsibility for this failure and profoundly undermines the "one country, two systems" model.

The Degraded Criminal Justice Process Under the NSL

---

[6] "Hong Kong Dumped from Economic Freedom List It Had Dominated," Bloomberg, March 3, 2021, https://www.bloomberg.com/news/articles/2021-03-04/hong-kong-dumped-from-economic-freedom-index-it-used-to-dominate ; and World Justice Project, Rule of Law Index, https://worldjusticeproject.org/rule-of-law-index

[7] See Generally, Michael C. Davis, *Making Hong Kong China: The Rollback of Human Rights and the Rule of Law* (Columbia University Press, 2021). https://cup.columbia.edu/book/making-hong-kong-china/9781952636134

[8] National People's Congress of the People's Republic of China (PRC), "The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region," June 30, 2020, https://www.elegislation.gov.hk/doc/hk/a406/eng_translation_(a406)_en.pdf.

With four vague crimes—secession, subversion, terrorist activities, and collusion with foreign forces—regulating speech in one form or another, the NSL represents a frontal attack on freedom of expression and political opposition in Hong Kong. These four crimes apply worldwide to both residents and non-residents, for actions both inside and outside Hong Kong. Hong Kong people and the city's friends abroad have watched in horror as people representing the city's leading voices for democracy and the rule of law have been arrested or forced to flee into exile. The reach of this oppression has included street protesters, the media, academics, the arts, and opposition politicians, with well over a hundred arrests in the first year of the NSL.

The parade of prosecutions began on the very first day of the NSL, with the arrest of Tong Ying Kit, a young protester who recklessly drove his motorcycle into cordons of police. His has been the first and only case so far to go to trial. In what appeared to be a reckless driving case, he was convicted for incitement to secession for carrying a flag with the popular slogan, "Liberate Hong Kong, Revolution of our Times." A special three judge panel of NSL designated judges found him guilty, based on his alleged intent to promote independence.[9] The court relied on a mere supposition that one possible meaning of the slogan was a call for independence. Although both the Basic Law and Article 4 of the NSL call for continuing application of the ICCPR, the court did not address the generally applicable human rights standard for incitement, that a speaker intend imminent violence and that such imminent violence be likely to occur. His reckless vehicle operation landed him a further conviction for terrorism, receiving a sentence of 9 years in total.[10]

Nearly all the remaining NSL cases involve political speech alone. Among the most notorious has been the prosecution of the prominent publisher of the Apple Daily, Jimmy Lai for collusion with foreign forces, presumably based on publications attacking the NSL and encouraging foreign pressure on Hong Kong. Several of his administrative staff and editors were likewise arrested. Mr. Lai languishes in jail after a bail denial that went all the way to the Court of Final Appeal.[11] The police raided his newspaper and eventually forced it to close by freezing its assets.

Perhaps, most shocking in the parade of NSL cases is the prosecution of nearly the entire active political opposition, asserting that participation in a July 2020 opposition-organized primary election amounted to conspiracy to subversion. Like political primaries everywhere, the opposition primary was designed to select the best candidates to run in the then planned September 2020 general election for the Legislative Council, an election that was later postponed at Beijing's

[9] *HKSAR v. Tong Ying Kit,* (2021) HKCFI 2200 (Hong Kong Court of First Instance, July 27, 2021). https://legalref.judiciary.hk/lrs/common/ju/ju_frame.jsp?DIS=137456&currpage=T

[10] See Michael C. Davis, "National security trial ruling a setback for human rights in Hong Kong," *South China Morning Post*, August 4, 2021. https://scmp.com/comment/opinion/article/3143634/national-security-trial-ruling-setback-human-rights-hong-kong

[11] *HKSAR v. Lai Chee Ying*, Final Appeal No. 1 of 2021 (Hong Kong Court of Final Appeal, February 9, 2021), https:/ https://scmp.com/comment/opinion/article/3143634/national-security-trial-ruling-setback-human-rights-hong-kong /legalref.judiciary.hk/lrs/common/ju/ju_frame.jsp?DIS=133491. For an analysis of the court's decision and the difficult strategic position it faced, see Simon Young, "Hong Kong's Highest Court Reviews the National Security Law—Carefully," *Lawfare*, March 4, 2021. https://www.lawfareblog.com/hong-kongs-highest-court-reviews-national-security-law-carefully#

direction.[12] Of the 47 being charged, 36 would languish in jail for months after bail denial.[13] The accusation of conspiracy to subversion relates to the plan by some opposition politicians, if they win a majority in the Legislative Council, to use a Basic Law provision respecting budget approval to force resignation of the Chief Executive. It seems only in Hong Kong does trying to defeat the government in accordance with constitutional requirements amount to subversion.

The repressive policies that animate the NSL, which on its face has no retroactive application,[14] extend well beyond the NSL itself. This has included the pre-existing public order laws, with the relentless prosecution of over 2,500 protesters from the 2019 protests. Prosecutions under these prior public order laws have targeted several senior opposition politicians, who during the 2019 protests were among the prime advocates that protesters stick to peaceful non-violent discipline. Among those convicted were the prominent barrister and Hong Kong's "father of democracy" Martin Lee. Mr. Lee was given an 11-month sentence, suspended for two years, while several of his colleagues were sent to jail.[15] Even the old British sedition law that had not been used in decades, has been resurrected to apply to statements made prior to the NSL.

The NSL suffers from much more than vague language. It represents a comprehensive threat to Hong Kong's autonomy, rule of law and basic freedoms. One would be hard-pressed to devise a more comprehensive plan to shut down an open society and inhibit the free-wheeling debate that has long characterized Hong Kong. Imposed without any public consultation, the NSL effectively stands above the Basic Law. The Hong Kong Court of Final Appeal (CFA) made this clear in the above noted denial of bail in the Jimmy Lai case, refusing to overturn the NSL's presumption against bail, which runs contrary to the common law presumption of innocence that has long prevailed in Hong Kong. The CFA expressly found it had no power to review the NSL for conformity to the Basic Law and that the bail provision is an exception to the usual rule.[16] Does this signal that any NSL deviation from human rights standards will be treated as an exception?

Other NSL provisions undermine Basic Law commitments to autonomy and the rule of law. Ignoring the legal requirements that mainland departments not interfere in Hong Kong affairs, the NSL creates both a Committee for Safeguarding National Security and an Office for Safeguarding National Security, both under the direct supervision of the Central Government. The former is made up of local officials with a mainland national security adviser, while the latter is completely staffed by mainland pubic and state security officials. For both, deliberations are secret and not subject to judicial review.

---

[12] "Explainer: How a Primary Got Hong Kong Activists in Trouble," Associated Press, March 1, 2021, https://apnews.com/article/beijing-primary-elections-democracy-hong-kong-elections-ccda7eb61403f721ba8e56423203f72a.

[13] NSL Article 42 creates a presumption against bail, contrary to the usual common law rule.

[14] NSL, Articles 39 and 66.

[15] Hong Kong pro-democracy figures given jail terms of up to 18 months," *The Guardian*, April 16, 2021. https://www.theguardian.com/world/2021/apr/16/jimmy-lai-martin-lee-hong-kong-pro-democracy-figures-sentenced

[16] Supra note 11, *HKSAR v. Lai Chee Ying*, Final Appeal No. 1 of 2021.

The NSL likewise creates special national security branches in both the police and the Department of Justice, which operate in secrecy and whose heads are appointed on the advice of the mainland Office for Safeguarding National Security. One of the first tasks carried out by the Committee for Safeguarding National Security was to issue special regulations for police operations under the NSL. These regulations allow for warrantless searches, surrender of travel documents, seizure and confiscation of property, interception of communications and secret surveillance.[17] It would appear that Hong Kong's newly minted secret police, both in the mainland Office for Safeguarding National Security and in the local special branches have a pretty free hand to conduct surveillance and target opposition figures with little chance of judicial oversight.

The Courts and Legal Profession Under Stress

Judicial independence and oversight are likewise compromised. Reflecting Beijing's distrust of Hong Kong's historically independent judges, the NSL provides that only designated judges can hear NSL cases. If designated judges make any statement, presumably in court, that officials believe offend national security then they can be removed. The Secretary for Justice can also choose to withhold the right to a jury in High Court cases where juries are typically allowed and replace such jury with a three-judge panel, as was done in the above noted *Tong Ying Kit* case. Added to these structural limitations, has been open pressure on judges, as Beijing and its supporters may publicly attack judges who stand in the way of government efforts to deny bail or convict. In the Jimmy Lai bail case noted above, the mainland *People's Daily* condemned the granting of bail and offered a somewhat veiled threat that the NPCSC might intervene, or if the CFA granted bail, the case might be transferred to the mainland.[18] This would not be an idle threat.

On top of all the restraints and pressure on the courts, the NSL allows the transfer of certain complex cases to the mainland for prosecution. This would be determined by the Office for Safeguarding National Security with the permission of the Chief Executive, a permission sure to be given. In considering the significance of all these structural and procedural hurdles one should bear in mind the harsh NSL punishments at risk—ranging from 3 years to life.

Hong Kong's prized legal profession likewise feels pressure under the NSL. China's official *People's Daily* recently likened the Hong Kong Bar Association to "street rats" and warned the Law Society to stay out of politics ahead of its leadership election—a view sadly echoed by the

[17] "Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region Gazetted," Government of the Hong Kong Special Administrative Region, Press Release, July 6, 2020, https://www.info.gov.hk/gia/general/202007/06/P2020070600784.htm

[18] In the article, translated in the People's Daily Observer, the leading state-run newspaper, after condemning Jimmy Lai as a dangerous criminal highlighted the mainland authorities' power to transfer such a complex case to the mainland for trial, surely signaling an intention to do so if the bail was not revoked on appeal. See, Su Di, "Observer: Approving Jimmy Lai's bail harmful to Hong Kong's rule of Law," *People's Daily*, December 28, 2020. https://peoplesdaily.pdnews.cn/opinions/observer-approving-jimmy-lai-s-bail-harmful-to-hong-kong-s-rule-of-law-190555.html

Hong Kong Secretary for Justice.[19] The Bar Association is widely respected for carrying out its responsibility to defend the rule of law. The president of the Hong Kong Bar Association, Paul Harris, was repeatedly attacked in mainland media when he had the temerity to suggest revision of the NSL to bring it in line with Basic Law requirements.[20] The representative of the legal functional sector in the Legislative Council, Dennis Kwok, was likewise repeatedly attacked for using legislative maneuvers to block enactment of a national anthem law. Mr. Kwok was eventually expelled from the Legislative Council and has since fled into exile.[21] All of the remaining opposition legislators resigned in protest after Kwok and three other lawmakers were expelled.[22] Professor Johannes Chan, a senior barrister and the former Law Dean at the University of Hong Kong, likewise came under withering attack when he defended the Student Union's free speech right after they passed a resolution of condolences and sympathy for the perpetrator of an attack on a police officer, the perpetrator having later committed suicide.[23] More recently four of the Student Union leaders have been arrested, accused of inciting terrorism in the resolution.

Lawyers were quite active in providing representation for the 2019 protesters and advocating more generally for upholding basic rights. In the face of attacks on other civil society groups, such groups as the Progressive Lawyers Group and the 612 Humanitarian Relief Fund (which provided legal assistance and other support to arrested protesters) have disbanded.[24] Even academic lawyers who have generally spoken out on human rights issues have, with few exceptions, largely gone silent. I have found I receive more calls overseas from the media because journalists find more difficulty finding legal experts willing to offer expert comment on human rights issues.[25]

---

[19] "Hong Kong's Justice Sec. warns law societies to steer clear of politics after Chinese state media blasts barristers," *Hong Kong Free Press*, August 16, 2021. https://hongkongfp.com/2021/08/16/hong-kongs-justice-sec-warns-law-societies-to-steer-clear-of-politics-after-chinese-state-media-blasts-barristers/

[20] "Beijing's top office in Hong Kong ratchets up attack on Bar Association chief Paul Harris, denouncing him as an 'anti-China politician'," *South China Morning Post*, April 25, 2021. https://www.scmp.com/news/hong-kong/politics/article/3131025/beijings-top-office-hong-kong-ramps-attack-bar-association

[21] For a careful analysis of the constitutional difficulties of the disqualifications see, Thomas E. Kellogg, "Beijing unbound: Hong Kong's autonomy crumbles as China rewrites the law," *Hong Kong Free Press*, November 17, 2020. https://hongkongfp.com/2020/11/17/beijing-unbound-hong-kongs-autonomy-crumbles-as-china-rewrites-the-law/

[22] "Hong Kong opposition lawmakers all quit after four members ousted," *The Guardian*, November 11, 2020. https://www.theguardian.com/world/2020/nov/11/china-pro-democracy-hong-kong-lawmakers-opposition-oust

[23] "Outspoken Hong Kong law professor Johannes Chan 'has left post at end of HKU contract,'" *South China Morning Post*, July 9, 2021. https://scmp.com/news/hong-kong/politics/article/3140496/outspoken-hong-kong-law-professor-johannes-chan-leaves-post

[24] The Progressive Lawyers Group has long focused on advocacy for human rights and the rule of law, while the 612 Humanitarian Relief Fund has focused on legal defense and support for arrested protesters. "Security Law: At least 8 Hong Kong pro-democracy groups disband in past 2 weeks, including lawyer's group," *Hong Kong Free Press*, July 6, 2021, https://hongkongfp.com/2021/07/06/security-law-at-least-8-hong-kong-pro-democracy-groups-disband-in-past-2-weeks-including-lawyers-group/ ; "Humanitarian fund helping arrested Hong Kong Protesters will halt operations by October 31," *Hong Kong Free Press*, August 18, 2021. https://hongkongfp.com/2021/08/18/humanitarian-fund-helping-arrested-hong-kong-protesters-will-halt-operations-by-october-31/

[25] "Why are Hong Kong academics quitting newspaper columns, and what's the fear over new 'red lines'? Three words: national security law," *South China Morning Post*, June 24, 2021. https://scmp.com/news/hong-kong/politics/article/3138478/why-are-hong-kong-academics-quitting-newspaper-columns-and

Undercutting Academic Freedom

Beijing has long been unhappy with Hong Kong's youthful opposition and has sought to impose a more patriotic brand of education, presumably to drain away youthful support for popular protests. In 2012, long before the imposition of the NSL, at Beijing's encouragement, the government had put forth proposals for national education.[26] They seemingly reasoned that liberal education was the basis for public support of the massive protests in 2003 and 2004 and a somewhat smaller protest over a high-speed rail in 2009. The government's 2012 national education proposal clearly backfired, generating even more political opposition. The proposal proved to be the impetus for the 2012 mass youth protests against brainwashing. Again, the government eventually backed down, but this protest had already given rise to a new generation of youthful protesters, some then as young as 14. As in 2003, the 2012 protest against patriotic education would lead to further later protests over democracy in the 2014 Umbrella Movement.

Beijing has built its long-standing education concerns into the NSL. Under NSL Article 9, the Hong Kong government is responsible "to take necessary measures to strengthen public communication, guidance, supervision and regulation…relating to schools, universities, social organizations, the media, and the internet.[27] Under Article 10, it is to "promote national security education in schools and universities and through social organizations, the media, the internet and other means…"[28] The government has already issued regulations requiring schools at all levels to teach national security, and various official statements have warned universities and the media about possible violations.[29] Beijing's official media have already attacked professors who speak out as "reactionary academics" and even Beijing supporters could find themselves branded as "loyal rubbish."[30] University leadership has offered no resistance to government directives. A culture of fear and self-censorship prevails on university campuses.[31]

The culture of intimidation is sometimes targeted directly at students. The ruling Hong Kong University Council, overriding academic discipline procedures, barred the above noted student leaders from campus after officials condemned their resolution of condolences over the suicide of

---

[26] Keith Bradsher, "Hong Kong Retreats on 'National Education' Plan," *New York Times*, September 8, 2012, https://www.nytimes.com/2012/09/09/world/asia/amid-protest-hong-kong-backs-down-on-moral-education-plan.html.

[27] "In Full: Official English Translation of the Hong Kong National Security Law," Article 9.

[28] "In Full: Official English Translation of the Hong Kong National Security Law," Article 10.

[29] Education Bureau of Hong Kong, "Education Bureau Circular No. 2/2021: National Security Education in School Curriculum - Implementation Mode and Learning and Teaching Resources," February 4, 2021, https://applications.edb.gov.hk/circular/upload/EDBC/EDBC21002E.pdf ; and Education Bureau of Hong Kong, "Education Bureau Circular No. 3/2021: National Security: Maintaining a Safe Learning Environment Nurturing Good Citizens," February 4, 2021, https://applications.edb.gov.hk/circular/upload/EDBC/EDBC21003E.pdf. The University Grants Council has already sent letters to public universities warning of the need for courses on national security at the risk of funding losses. Mimi Leung and Yojana Sharma, "Universities pressed to implement 'security law' education," *University World News*, March 24, 2021. https://www.universityworldnews.com/post.php?story=20210324074153521

[30] Au Ka-lun, "A new Cultural Revolution is on its way," *Apple Daily*, March 26, 2021. https://hk.appledaily.com/opinion/20210326/GDMGSIJ2AVBOLLW7QC5BUJUBY4/

[31] "As Hong Kong Law Goes After 'Black Sheep,' Fear Clouds Universities," *The New York Times*, November 7, 2020. https://www.nytimes.com/2020/11/07/world/asia/hong-kong-china-national-security-law-university.html

the attacker. The university administration had already severed relations with the Student Union, which had passed and then later apologized for the resolution.[32]

With the local NSL education regulations in place, Beijing in mid-2021 targeted its wrath below the tertiary level at the Professional Teachers Union (PTU), accusing this 48-year-old teacher's labor union of being too political and the teachers themselves of brainwashing students against China. Reminiscent of mainland style political purges, both China's Xinhua news agency and the *People's Daily* in commentary referred to the 95,000 member PTU as a "malignant tumor."[33] The Hong Kong government then severed all relations with the union with which it had cooperated for decades, and the police announced a criminal investigation. This led to the union's decision in August 2021 to disband. Beijing officials have made clear that leading members should still be pursued. These attacks on academic freedom in Hong Kong have left their mark, with the Global Public Policy Institute giving Hong Kong a D-rating on academic freedom in its global survey.[34]

Civil Society Organizations Under Severe Pressure

A broad spectrum of civil society and labor organizations are also feeling the heat, with organizations such as the Labor Party, the Confederation of Trade Unions, the Social Workers General Union, the League of Social Democrats, and the Hong Kong Alliance in Support of the Patriotic Democratic Movement in China (which had organized the June 4th vigils every year until such vigils were banned) often the target of official condemnation. The most recent target was the Civil Human Rights Front. Speculation is that that the Confederation of Trade Unions, which gathers trade unions under one umbrella, will likely be the government's next target.

The Civil Human Rights Front (CHRF), which for 19 years had been an umbrella organization uniting many pro-democracy organizations in organizing public protests, has especially came under severe pressure. It had for years cooperated with government to submit proper applications for the many peaceful protest marches it organized and was noted for its insistence on non-violent strategies. On December 10, 2019, when I interviewed one of its leaders, this leader described their efforts that day to organize one of the first protests permitted on Hong Kong Island in recent months. They had persuaded the police that if aggressive enforcement tactics were not used, they expected the protest would come off without violence—as in fact occurred. But official tolerance changed dramatically in 2021: first, in March rumors surfaced that the police were investigating the front under the NSL; in May the then convenor of the organization, Figo Chan Ho-wun, was jailed for 18 months for participating in a 2019 unauthorized protest; then Beijing's Hong Kong and Macau Affairs Office accused the organization of colluding with foreign forces and attempting

[32] "University of Hong Kong bypassed normal disciplinary procedure in banning student leaders from campus, insiders say," *South China Morning Post*, August 3, 2021. https://www.scmp.com/news/hong-kong/politics/article/3143884/university-hong-kong-bypassed-normal-disciplinary-procedure

[33] ""Hong Kong's biggest teachers' union 'seeks to speed up dissolution by changing its rules' as Beijing attack continue," *South China Morning Post*, August 11, 2021. https://scmp.com/news/hong-kong/politics/article/3144711/hong-kongs-biggest-teachers-union-seeks-speed-dissolution

[34] "Hong Kong's Global Academic Freedom Index regresses C-level to D-level, lower than Vietnam, causing concern," *Apple Daily*, April 2021. https://hk.appledaily.com/international/20210316/TNKQG3RI2VBDBOKXGFEJBLY7AY/?utm_source=HRIC+Updates&utm_campaign=686911b077-HRIC_DAILY_BRIEF_COPY_01&utm_medium=email&utm_term=0_b537d30fde-686911b077-259232682

to stage a "color revolution;" and, finally, under Beijing pressure, the police repeatedly signaled their intention, even after the organization folded, to investigate the group's leaders for criminal behavior. This led to several organization, including the above-noted PTU withdrawing from the front. Under pressure, the CHRF announced that it had disbanded on August 13, 2021.[35]

Prominent overseas organizations such as Human Rights Watch, the US National Endowment for Democracy and affiliates, the Hong Kong Democracy Council and Amnesty International have also been attacked in state media and targeted for sanctions.[36] International businesses have not been immune from pressure. A recent survey by the American Chamber of Commerce in Hong Kong revealed that even 42 percent of its business members plan to leave the city.[37]

Media Censorship

Local news organizations, art exhibits and critical documentaries have also come under attack.[38] Most notorious in this regard was the above-noted systematic effort to shut down the leading opposition newspaper, the Apple Daily, first arresting its publisher, Jimmy Lai and several of his executives, charged with collusion under the NSL, then raiding the newspaper offices and eventually arresting several editors and freezing the papers assets. The last move brought the paper to an end and cost over 1000 workers their jobs.[39]

Even the independent public broadcaster, RTHK has been targeted, with the government putting in place a new Director of Broadcasting taken from the civil service to tame the broadcasters' coverage. Along the way several reporters were dismissed, and documentary and public affairs shows critical of the government or of the police were cancelled. In the latest move RTHK is being partnered with Chinese state media, CCTV, as Hong Kong Chief Executive Carrie Lam put it, to

---

[35] "Hong Kong protests: Civil Human Rights Front confirms it has disbanded as members steer clear amid police investigation," *South China Morning Post*, August 15, 2021, https://scmp.com/news/hong-kong/politics/article/3145093/hong-kong-protests-civil-human-rights-front-confirms-it ; "From fledgling alliance toprotest powerhouse: A tumultuous 19 years for Hong Kong's Civil Human Rights Front," *South China Morning Post*, August 15, 2021. https://scmp.com/news/hong-kong/politics/article/3145116/fledgling-alliance-protest-powerhouse-tumultuous-19-years

[36] Selina Cheng, "Premier Hong Kong protest coalition comes under fire from pro-Beijing and state media, leader vows to continue," *South China Morning Post*, March 19, 2021. https://hongkongfp.com/2021/03/19/premier-hong-kong-protest-coalition-comes-under-fire-from-pro-beijing-and-state-media-leader-vows-to-continue/

[37] "Security Law: US business group warns 42% of members plan Hong Kong exit, as police chief issues warning on 'fake news'," *Hong Kong Free Press*, May 12, 2021. https://hongkongfp.com/2021/05/12/security-law-us-business-group-warns-42-per-cent-of-members-plan-hong-kong-exit/

[38] HG Masters, "Hong Kong Arts Sector Faces New Political Scrutiny," *ArtAsiaPacific,* March 18, 2021. http://www.artasiapacific.com/News/HongKongArtsSectorFacesNewPoliticalScrutiny ; "Hong Kong's Lam vows 'full alert' for art endangering national security, as artist warns of 'devastating' crackdown," *Hong Kong Free Press*, March 17, 2021. https://hongkongfp.com/2021/03/17/hong-kongs-lam-vows-full-alert-against-artworks-endangering-national-security-as-artist-warns-of-devastating-crackdown/ ; Candice Chau, "Hong Kong campus protest documentary screening cancelled hours before showing following attack by pro-Beijing paper," *Hong Kong Free Press*, March 15, 2021. https://hongkongfp.com/2021/03/15/hong-kong-campus-protest-documentary-screening-cancelled-hours-before-showing-following-attack-by-pro-beijing-paper/

[39] "What next for the workers laid off at Hong Kong's Apple Daily?" *China Labor Bulletin*, August 10, 2021. https://clb.org.hk/content/what-next-workers-laid-hong-kong's-apple-daily

air more programs to "nurture a stronger sense of patriotism" among viewers.[40] Lam also announced that RTHK will produce its own programing on the importance of national security. The Chair of the Hong Kong Journalist Association (HKJA), Ronson Chan, worries that this public broadcaster, created in the image of the BBC, is quickly being turned into a state propaganda mouthpiece. Chan expressed doubt most Hong Kong people would watch such programming.

The HKJA is itself at risk and reasonably fears it will be next on the list of organizations forced to disband. The Beijing controlled Wen Wei Po newspaper has already attacked it as an "anti-government political organization."[41] The paper accused the HKJA of "wantonly smearing the Hong Kong government, the police and the national security law." HKJA's chair defended the organization's role of defending its member and press freedom.

Other signs of the closing media space abound. Perhaps the most notorious free speech case, beyond the closing of the Apple Daily, has been the arrest of two speech therapists, Lai Man-ling and Melody Yeung, along with three other members of the General Union of Hong Kong Speech Therapist, for simply publishing a children's book about sheep being under attack by wolves.[42] Presumably the Hong Kong and Beijing governments presume they are the wolves. National security police have also been monitoring the internet. The police closed a website called HKChronicles, that was dedicated to publishing first-hand accounts of the 2019 protests, claiming the power to monitor such under NSL article 43.[43]

The Office for Safeguarding National Security, under NSL Article 54, is afforded similar oversight over foreign NGOs and news agencies. The obvious risk early on caused the New York Times to move some of its operations out of Hong Kong.[44] With such vague laws, these forms of oversight reach across the society and leave considerable uncertainty as to what is prohibited and what is not. They clearly aim to have a chilling effect on media voices in opposition to the government. These policies and prosecutions have met with international condemnation.[45]

Degrading the Democratic Process

[40] "Hong Kong's RTHK will become state media after partnership with China's CCTV, says press group chief," *Hong Kong Free Press*, August 11, 2021. https://hongkongfp.com/2021/08/11/hong-kongs-rthk-will-become-state-media-after-partnership-with-chinas-cctv-says-press-group-chief/

[41] "Beijing-controlled paper labels Hong Kong press union an 'anti-govt political organization," *Hong Kong Free Press*, August 13, 2021. https://hongkongfp.com/2021/08/13/beijing-controlled-paper-labels-hong-kong-press-union-an-anti-govt-political-organisation/

[42] "Hong Kong women who 'published seditious children's books about sheep' remanded in custody," *Hong Kong Free Press,* July 23, 2021. https://hongkongfp.com/2021/07/23/hong-kong-women-who-published-seditious-childrens-books-about-sheep-remanded-in-custody/

[43] "Hong Kong police use national security law for first time to block access to website anti-government protests, officer' details," *South China Morning Post*, January 9, 2021. https://www.scmp.com/news/hong-kong/law-and-crime/article/3117072/hong-kong-police-use-national-security-law-block

[44] "New York Times Will Move Part of Hong Kong Office to Seoul," *New York Times*, July 14, 2020. https://www.nytimes.com/2020/07/14/business/media/new-york-times-hong-kong.html

[45] 2021 Hong Kong Policy Act Report, US Department of State, Bureau of East Asian and Pacific Affairs, March 31 2021. https://www.state.gov/2021-hong-kong-policy-act-report/

If the intention to exclude all opposition to the government were not clear enough, it was made even more clear in March 2021 when Beijing again intruded directly on the Hong Kong system to amend the electoral provisions in Annexes I and II of the Basic Law.[46] Under the amendments issued by the NPCSC on March 30, 2021, the previous Beijing-friendly 1200-member Election Committee that chose only the chief executive was expanded to 1500 members. This committee, whose members are to be chosen mostly by pro-Beijing forces via a small circle election of functional and official sectors, vetted as "patriots," will have the responsibility to vet and nominate all candidates both for chief executive and the Legislative Council, as well as elect the chief executive and nearly half of the legislative counsellors.

Beijing has carefully stacked this powerful Election Committee with its loyalists. The shift from 1200 to 1500 members is achieved by adding 300 new members from top-down Beijing appointed bodies who supposedly represent Hong Kong in the central government. This creates a major conflict of interest with, in many cases, current officials choosing or recommending people who may later re-elect them. 117 District Counsellors, who sat on the previous Election Committee have been replaced by representatives of various loyalist organizations. Corporate voters and other pro-Beijing forces dominate most of the remainder of the Election Committee, with further possible conflicts of interest implicated. In some cases, the amendments require that a portion of the candidates from some functional sectors be nominated by mainland affiliated organizations such as, for example, the China Law Society or the Chinese Academy of Sciences.

It is widely believed that Beijing took these drastic actions against democratic development because its favored candidates were roundly defeated in the 2019 District Council (DC) elections, with oppositions candidates taking 90 percent of the seats. The DC has very little power, but it is the only level where most seats were directly elected. Both Beijing and the opposition had cast the 2019 DC election as a referendum to show opposition to or support for protest demands. The support camp clearly won. The Hong Kong government then moved to disqualify the elected opposition counsellors based on a planned oath and loyalty test, resulting in most eventually resigning to avoid investigations and possible charges.[47]

The new election law, both in the Beijing template, and the local law enacted to carry it out, will effectively bar the pan-democratic camp from the political process. In its first outing, Beijing's attempt to paint this model as democratic was quickly rebutted at the close of candidate registration for the Election Committee in August 2021 when it was reported that 75 percent of those registering for the small circle election to this powerful election body would be running unopposed.[48] The mainland electoral system had arrived in Hong Kong, there being barely more

[46] NPCSC, "Method for Selection of the Chief Executive of the Hong Kong Special Administrative Region," *Hong Kong Basic Law, Annex 1, http://www.xinhuanet.com/english/download/2021-3-30/AnnexI.pdf* ; NPCSC, "Method for the Selection of the Legislative Council of the Hong Kong Special Administrative Region, Hong Kong Basic Law, http://www.xinhuanet.com/english/download/2021-3-30/AnnexII.pdf (hereinafter "Amended Basic Law Annexes")
[47] "'Ten thousand apologies': Dozens of pro-democracy district councillors step down amid reports of impending disqualifications," *Hong Kong Free Press*, July 8, 2021. https://hongkongfp.com/2021/07/08/ten-thousand-apologies-dozens-of-pro-democracy-district-councillors-step-down-amid-reports-of-impending-disqualifications/
[48] "Record number of uncontested seats for Hong Kong Election Committee polls—and Li Kashing is not throwing his hat into the ring, for the first time since 1997," *South China Morning Post*, August 12, 2021.

candidates than there were seats available. It seems the old saw, that Beijing officials do not mind elections, as long as they know the outcome ahead of time is being proven.

One need only look at the onerous process to vet candidates for loyalty to understand why there is little opposition interest in participating in upcoming elections. Beyond the vetting done by the Election Committee, the amendments also establish a small Candidate Eligibility Review Committee to separately vet all political candidates for office in the territory. That small committee is dominated by officials and long-tested pro-Beijing figures. The review committee will in turn be advised by the Committee for Safeguarding National Security set up under the NSL, which in turn will be supported by investigations of every candidate by the national security police unit. Such investigations will be conducted in secret and the candidates will reportedly not be told why they are denied candidacy—rendering the choice to run for office a risky proposition with major privacy concerns. The new provisions also provide there will be no appeal of any disqualification.

The chances of an opposition candidate clearing all these hurdles and getting elected in most of the small-circle Beijing-friendly constituencies is nil. The Election Committee historically has been so stacked with Beijing loyalists that opposition candidates running for chief executive could muster at most about 20% of the committee's votes. The projected changes will reduce the number of committee members that might favor the opposition, either for electing the chief executive or for nomination or election to the 40 legislative seats controlled by the Election Committee.

Under the Basic Law amendments, the total seats in the Legislative Council will be increased from 70 to 90 members, but the number of directly elected seats will be nearly cut in half, from 35 to only 20. The functional sectors, crafted to ensure pro-Beijing control, will have 30 seats and the remaining 40 seats will be chosen by the Election Committee. It is too early to tell if opposition candidates will even bother to run in this new highly vetted system. For the Election Committee itself, at the close of nomination none had. Even for the minority of 20 directly elected seats, with no genuine choice, voters may not bother to vote or perhaps may boycott the elections. To avoid a campaign to submit blank ballots or not vote in the Legislative Council election the government has already passed a local law making advocacy of a boycott or blank voting illegal, though a voter doing either on their own is perfectly legal. International condemnation has already flowed in.[49]

While the NSL largely uses intimidation to silence opposition, the new election laws will effectively block opposition politicians from office. A variety of other detailed limitations make it highly unlikely opposition candidates will participate in elections. Most, by virtue of the massive NSL prosecutions, will have little likelihood of qualifying. Any who have somehow escaped prosecution would judge their support in these heavily stacked bodies so insignificant that they

https://scmp.com/news/hong-kong/politics/article/3144856/hong-kong-politics-record-number-uncontested-seats-election

[49] "Election revamp: Urging people not to vote or spoil ballots may be criminalized, even without proof of intent to sabotage poll," *Hong Kong Free* Press, April 23, 2021. https://hongkongfp.com/2021/04/23/election-revamp-urging-people-not-to-vote-or-spoil-ballots-may-be-criminalised-even-without-proof-of-intent-to-sabotage-poll/ See also, Antony J. Blinken, Secretary of State, "Assault on Democracy in Hong Kong," Press Statement, March 11, 2021. https://www.state.gov/assault-on-democracy-in-hong-kong/

would reasonably conclude it not worth the loss of privacy and possible risk of prosecution to run.

International Policy Initiatives

In the couple years since the 2019 crackdown against protesters began foreign governments have tried a number of strategies to sway China to return to its commitments in Hong Kong. In the US this began with enacting the Hong Kong Human Rights and Democracy Act. This was quickly followed with the withdrawal of the recognition of Hong Kong's special status, as had previously been upheld under the Hong Kong Policy Act. Since then, a variety of legislation and executive orders have sought to ease the path for Hong Kong residents and activists to seek refuge in the US.[50] These strategies were supplemented by targeted sanctions on individual officials in Hong Kong and Beijing. In its era of "great power" and "wolf warrior" diplomacy,[51] Beijing has shown no inclination to heed these expressions of international concern. Rather it has tended to escalate its interventions in Hong Kong.

Other strategies, encouraged under the Biden administration, have invoked human rights and democracy more broadly and have encouraged the strengthening of related alliances, consistent with widely shared global values. There also appears to be growing appreciation of the need for the United States to get its own house in order, in terms of policies related to the democratic processes, infrastructure and the global environment. Multi-lateral work with partners, the United Nations or other international governmental organizations work best when consistent with domestic policies. International institutions can serve as vehicles to express shared values in resolutions and fact-finding, and for setting guidelines for participation and applying appropriate pressures where needed.[52] When criticisms targeting China's human rights violations or aggressive policies have only been unilateral, China has often responded with the usual whataboutism arguments about the US's own failings. A multilateral approach that encourages participation in shared norms may be more effective. At the same time, it will be important to sort out ways to use economic incentives to encourage compliance.

Within this broader context, the impact of sanctions on Beijing's policies in Hong Kong has been negligible. China has continued its harsh crackdown on the opposition in Hong Kong. Beijing recently indicated plans to extend the national Anti-Foreign Sanctions Law to Hong Kong, though this was put on hold in the late August NPCSC meeting. If that plan is taken up again the law will presumably be added to Annex III of the Basic Law, with further enactment of local

[50] Since Samuel Chu and the Hong Kong Democracy Council have been directly involved with various legislative initiatives, I will assume Samuel Chu will discuss these in greater detail.
[51] China Media Project, "Growling Back at the West," August 8, 2021. https://chinamediaproject.org/2021/08/08/growling-back-at-the-west/
[52] "National security law: UN rights official calls on Beijing to allow fact-finding mission to Hong Kong," *South China Morning Post*, July 2, 2021. https://scmp.com/news/hong-kong/politics/article/3139525/national-security-law-un-rights-official-calls-beijing ; Activists urge UN official to visit Hong Kong and investigate 'disappearance of freedoms' under security law," *Hong Kong Free Press*, July 2, 2021. https://hongkongfp.com/2021/07/02/activists-urge-un-officials-to-visit-hong-kong-and-investigate-disappearance-of-freedoms-under-security-law

legislation. This local law, as in the national law, would presumably sanction foreign officials, entities, or individuals worldwide who act to enact or carry out foreign sanctions against China. The national law includes in its tool kit denials of visas, asset seizures and deportation. It also opens the door to civil actions by Chinese companies hurt by a foreign company that executes foreign sanctions. While the offending actions can occur anywhere, the property or individuals reached must be in China. Both passing this law on the mainland and putting it on hold in Hong Kong shows China's heightened sensitivity to foreign initiatives that may have an economic impact. The elements of required reporting and allowance of civil suits over foreign sanctions highlights the centrality of concern over economic isolation.

One possible move that might deflect such a tit-for-tat response, would be for the US to emphasize the importance of human rights and the rule of law as a central US policy concern and then to build that concern more systematically into our commercial regulatory regime and foreign policy outreach. Couching US policy as sanctions may simply invite an equal response. Multilateral alliances and agreements can be used to address human rights concerns more effectively, even if the realization of the policy objectives may be less immediate.

Of course, Hong Kong people cannot wait for the US or international community to get their house in order regarding these important priorities. The short-term response should be focused on immigration, to afford both Hong Kong protesters and ordinary people an escape. In the face of hopelessness, the response to this extraordinary crackdown is becoming clear, the exit of Hong Kong's best and brightest, reportedly at the rate of about 1000 per day.[53]

In this age of the aging labor force there is great self-serving advantage to welcoming Hongkongers fleeing tyranny to our shores. But in terms of our human rights and rule of law priorities such offer of a haven is imperative. President Biden has announced an 18-month visa extension, with permission to work, for Hongkongers already in the US. I would suggest this allowance be extended to allow conversion to permanent residence and citizenship. I would further suggest the US follow Canada in allowing a path to permanent residence for Hongkongers completing degrees at US universities.[54] The US could only benefit from acquiring such talent and a lot of the activism in Hong Kong was centered in universities. Opening our academic door to students leaving Hong Kong could be a path to citizenship.

---

[53] "Hong Kong experiences 'alarming' population drop, but government says not all 90,000 leaving city because of national security law," *South China Morning* Post, August 12, 2021. https://www.scmp.com/news/hong-kong/society/article/3144845/hong-kongs-experiences-alarming-population-drop-government Jason Wardie, opinion, "The current exodus from Hong Kong isn't like pre-1997—these people won't be returning. And that changes the city," *South China Morning Post*, July 22, 2021. https://www.scmp.com/magazines/post-magazine/article/3141995/current-exodus-hong-kong-isnt-pre-1997-these-people-wont-be

[54] "Two new paths to permanent residence launched for Hongkongers in Canada as minister cites 'deteriorating human rights situation,'" *Hong Kong Free Press*, June 9, 2021. https://hongkongfp.com/2021/06/09/two-new-paths-to-permanent-residence-launched-for-hongkongers-in-canada-as-minister-cites-deteriorating-human-rights-situation/

OPENING STATEMENT OF ANGELI DATT, SENIOR RESEARCH ANALYST FOR CHINA, HONG KONG, AND TAIWAN, FREEDOM HOUSE

VICE CHAIRMAN CLEVELAND: Regrettably real. Thank you, very much. Ms. Datt?

MS. DATT: Thank you, Commissioners for convening this very timely and important hearing and for inviting me to speak about the impact of the National Security Law on media and internet freedom in Hong Kong.

In my remarks this morning, I'll focus first on Hong Kong's internet and media space as closing yet remains different from mainland China's. Second, the long-term prospects for these rights under the National Security Law. And finally, recommendations for how the U.S. government and Congress can respond.

The crackdown in Hong Kong after Beijing imposed the National Security Law has significantly impacted media and internet freedom. It has many characteristics of the restrictive environment in mainland China. Several trends we are seeing in Hong Kong include arrests and attacks on journalists, the transformation of the public broadcaster Radio Television Hong Kong into state media, increased state or Mainland- linked actors ownership over media, and the use of administrative measures to restrict transparency and journalistic freedom.

In particular, the crackdown and closure of Apple Daily is emblematic of how the National Security Law is being used to stifle press freedom. It also reinforces the retroactive nature of the National Security Law. In the internet space, there's been an increase in website blocks, content removal and censorship, arrests for online activity, the surveillance of opposition figures, and cyberattacks. The specific details and cases of these trends are included in my written testimony.

I'll use the remainder of my time to focus on what is still different in Hong Kong and what to watch for. The U.S. Government and interested groups should pro-actively prepare for further crackdowns in Hong Kong and be ready to respond with a range of tools. Hong Kong is not dead, but the territory is nearly unrecognizable under the National Security Law. It is important to recognize how Hong Kong's media and internet space is still different from mainland China, though. Especially as these are areas to watch and protect from further restrictions.

First, journalists are still reporting critically on news events and independent media is still allowed to exist. Hong Kong media continues to report on and publish content that is banned on the mainland. Many of the sources from my written testimony come from journalists and outlets reporting from the city. Two, websites are by and large, not blocked. To date, only six websites have been blocked. This is vastly different from the mainland system where the great firewall currently blocks thousands of websites. And three, the distinction between self-censorship and government ordered censorship, with some exceptions, most content removal has largely come at the hands of publishers. However, the National Security Law grants police sweeping powers to order the content removed and police will continue to flex those powers. As this analysis has covered, emboldened Beijing has demonstrated it will continue to crack down on Hong Kong until there is no opposition left. The long-term prospects for information flow include the following areas to watch for further restrictions.

One, new legislation such as a proposed law on fake news and a bill recently introduced to ban doxing would result in further restrictions. Police have already threatened the press for arrest for so called fake news under the National Security Law. And any fake news law would be

wielded against critical outlets. The bill could result in the arrest of employees of technology companies, including American firms that host content the government orders to be removed.

Two, the forced sale or pressure to close independent media. The South China Morning Post, sometimes called Hong Kong's paper of record, faces the prospect of a sale to a Chinese state entity or individual and being turned into a propaganda outlet. Following the sale of the SCMP to Alibaba in 2016, there were already concerns about the paper's independence. The above mentioned independent and critical media outlets that still exist may have to relocate their headquarters away from Hong Kong or close altogether.

Three, eroding legal protections for the press, such as increased warrantless searches of journalistic material will put sources and journalists at risk, and will likely lead to more self-censorship.

And four, asset seizures under the National Security Law to silence critics. Police use of economic coercion directly led to the closure of Apple Daily, the sale of its Taiwanese sister paper, and the folding of its parent company Next Digital, which was the largest publicly listed media company in Hong Kong. The CCP essentially stripped a businessman of his assets and shut down his company because of his political views. The likely introduction of China's Anti Sanctions Law in Hong Kong will have further ramifications for businesses.

And five, crackdowns in Hong Kong will have a regional global impact on Chinese language media, which has traditionally counted some of Hong Kong's press amongst the independent credible news outlets available for the Chinese- speaking world.

Hong Kongers are living in a high-risk territory where they could face potential life in prison for exercising their human rights. Moreover, the impact of the crackdown is being felt far beyond the territory's borders, including here in the United States. Some of Freedom House's recommendations for further action include --

One, due to the change in ownership at Phoenix television as detailed in my written testimony, the Department of Justice should order the company to register its U.S. subsidiary under the Foreign Agents Registration Act, similar to action taken last month regarding the newspaper Sing Tao. Two, Congress should hold hearings with American tech companies and how the companies are preparing for further crackdowns in Hong Kong, including head of legislative elections in December, and how they will defend their users' digital rights. And three, the Biden administration should use humanitarian parole for Hong Kongers and Congress should pass legislation to ease and hasten entry into the United States for Hong Kongers being targeted for their peaceful involvement in human rights activities.

In conclusion, to put the dramatic assault on media freedom in Hong Kong under the National Security Law in perspective, let me share an analogy of what similar events would look like in the United States. In just over a year, the Washington Post shuts down and deletes its entire online presence. Jeff Bezos, and the entire post executive team and senior new staff are all in jail. BuzzFeed deletes all of its opinion articles out of fear of reprisals. National Public Radio deletes all of its content older than a year, pulls popular shows, and threatens to charge journalists for producing these shows. For Hong Kongers, or is this is the reality that they are contending with as Beijing dismantles their previously free society. Thank you again for holding this hearing and for giving me the opportunity to contribute my observations. I'm happy to expand on my testimony during the Q&A. Thank you.

PREPARED STATEMENT OF ANGELI DATT, SENIOR RESEARCH ANALYST FOR CHINA, HONG KONG, AND TAIWAN, FREEDOM HOUSE

The Impact of the National Security Law on Media and Internet Freedom in Hong Kong

Written Testimony by Angeli Datt
Senior Research Analyst for China, Hong Kong, and Taiwan at Freedom House

U.S.-China Economic Security Review Commission (USCC)
Hearing on "U.S.-China Relations in 2021: Emerging Risks"
September 8, 2021

Introduction

The national security arrests and subsequent closure of the *Apple Daily* newspaper in Hong Kong in June 2021 marked the lowest point for press freedom in the territory in recent memory. Under the new national security regime imposed by Beijing, journalists and news executives have been jailed and face life imprisonment for publishing articles. The paper's closure will be felt globally. The end of *Apple Daily* is just one of many examples demonstrating how much press freedom has changed in over a year in Hong Kong.

This testimony examines the shrinking space for media and internet freedom in Hong Kong since Beijing imposed the National Security Law (NSL) on the territory on June 30, 2020. The National Security Law prohibits a wide range of activities under the four main offenses of separatism, subversion, terrorism, and colluding with foreign forces, assigning a maximum penalty of life in prison. The NSL has rapidly transformed Hong Kong towards an authoritarian system, with serious implications for the future rights enjoyed by Hong Kong people, as well as for American and other foreign individuals and businesses operating in the territory.

Despite Article 4 of the NSL ostensibly safeguarding human rights, in practice the NSL created vaguely defined political red lines which infringe on those rights. This is a familiar tactic used by the authoritarian Chinese Communist Party (CCP) in mainland China. Such vague legal provisions create uncertainty and fear in the population, with detention and imprisonment imposed when the lines are crossed. Beijing's role in directly imposing the law effectively ended Hong Kong's autonomy and has infringed on human rights guaranteed under Hong Kong's Basic Law and international human rights laws in force in Hong Kong. While the people residing in Hong Kong are the main targets of the crackdown, the NSL also has global ramifications due to Hong Kong's center as a business hub and the NSL's extraterritorial jurisdiction, including against persons who are not permanent residents of Hong Kong.

To try and put the crackdown on media in Hong Kong into perspective for an American audience, an analogous situation is that in just over a year, the *Washington Post* would have shut

down and deleted its entire online presence after Jeff Bezos was arrested and his and the paper's parent company's assets frozen. The entire Post executive team and senior news staff would be in jail. Buzzfeed would have deleted all of its opinion articles out of fear of arrest. National Public Radio would have deleted all of its content older than a year, pulled popular programing, and threatened to charge journalists for producing those shows. For Hong Kongers, this is the reality they have to contend with as Beijing dismantles their previously free society.

Thank you for this opportunity to testify. After a short background on the situation in Hong Kong under the NSL, I have divided my remarks into five parts and ask that this full written testimony be admitted into the record:

1. Media freedom trends in Hong Kong under the National Security Law
2. Internet freedom trends in Hong Kong under the National Security Law
3. How Hong Kong's media and internet space remains different from mainland China
4. Long term forecasts on the media and internet space in Hong Kong
5. Recommendations for the US government and Congressional responses

Background

The crackdown in Hong Kong following the application of the NSL has demonstrated the CCP's intent to trample on human rights, the rule of law, and its domestic and international legal obligations to stifle expression or activities which it considers a challenge to its rule in the territory. This strategy has been acutely felt by those exercising their rights to political participation, freedom of expression, assembly, and association, and the press.

The government is restricting the right to participate in public affairs only to those who support the government, so called "patriots," according to CCP leader Xi Jinping,[1] with harsh punishments being meted out to government critics and opposition politicians. Forty-seven activists and politicians have been remanded in custody since February 2021 after being charged with "subversion" under the NSL for holding a primary election to select candidates who would represent the prodemocracy camp in Legislative Council elections, now scheduled for December 2021. They face potential life imprisonment. In March, Beijing dramatically altered Hong Kong's electoral system, with changes made to ensure the pro-Beijing camp consolidates control and that the opposition cannot gain seats. In the new system, only 20 out of the 90 Legislative Council seats will be directly elected (compared with 35 of 70 previously), corporations and professional groups will elect 30 members, and the unelected Election Committee will send 40 of its members. All candidates must undergo a screening process conducted by Hong Kong national security police and a government-appointed body.[2]

Freedom of expression online and offline has been under sustained attack and Hong Kongers have faced arrest and prosecution for political speech. For example, the first person convicted under the NSL, Tong Ying-kit, received a nine-year prison sentence in July 2021 for displaying a political slogan while driving dangerously.[3] Teenage activist Tony Chung has been arrested and charged under the NSL for "secession" over Facebook posts.[4] In July, five speech therapists were arrested on charges of "sedition" for writing a children's book.[5] The right to freedom of assembly has also been seriously curtailed in the aftermath of the 2019 prodemocracy protests.

Applications for permits to hold assemblies have been systematically denied under restrictions put in place on public health grounds ostensibly due to COVID-19 but extended to include political objections. As such, since the NSL came into effect, the annual Tiananmen vigil and July 1 protest have been banned.[6] There have also been several criminal convictions of individuals who took part in 2019 assemblies.[7]

The right to freedom of association has also been restricted, including threats against independent trade unions leading several to disband out of fear.[8] Civil society organizations that organized protests—often using online platforms—such as the Civil Human Rights Front, have disbanded under threat of prosecution for endangering national security.[9] Other CSOs disbanded due to fear of prosecution under the NSL. The largest teacher labor union disbanded after being labeled a "malignant tumor" by *The People's Daily*, the CCP's mouthpiece, which also attacked the Hong Kong Bar Association as a "running rat."[10]

Such is the intensity of the crackdown that thousands have chosen to leave their home, if they can. Population statistics show a drop of 90,000 people, or 1.2% of the population in the year after the NSL was enacted, the largest drop since 2003, and over 30,000 people applied for the UK's special visa for Hong Kongers within two months.[11] Some journalists have reported leaving Hong Kong out of fear.[12] New legal restrictions could create the kind of exit bans normally seen in mainland China.[13] In July 2021, a reporter for a US-based Chinese language publication had her travel documents seized and was barred from leaving Hong Kong after being placed under investigation under the NSL for filming a knife attack on police.[14]

1) Media freedom trends in Hong Kong under the National Security Law

Within one year after the adoption of the National Security Law (NSL), many predictions of its impact on press freedom have unfortunately come to pass. These include arrests of journalists, criminal penalties for critical news outlets, retroactive charges covering content released prior to the imposition of the NSL, and deterioration of digital freedoms.[15] This is despite attempts by Hong Kong chief executive Carrie Lam and Beijing officials in 2020 to reassure Hong Kongers that the law would target "an extremely small minority of illegal and criminal acts" and that the "basic rights and freedoms of the overwhelming majority of citizens will be protected."[16] Events of the past year have shown that this is not the case, with sweeping restrictions brought about by the NSL severely impacting press freedom and free expression of millions of Hong Kongers. Authorities now deploy a range of criminal penalties from NSL crimes, to colonial-era sedition crimes, to existing criminal legislation, to punish protected human rights activities, including independent journalism.

The implementation of the NSL has led to Hong Kong's press freedom dropping to its lowest level in decades. According to the Hong Kong Journalist Association (HKJA) 2021 annual report released in July, press freedom is in "tatters."[17] HKJA's Hong Kong Press Freedom Index released in May 2021 showed the lowest overall score on record since the association began publishing the index in 2013. The annual survey of journalists showed that 91 percent believe press freedom had worsened since the previous year.[18] Internet freedom has been reduced, albeit not to the same degree as attacks on media. Several of these changes are features of the mainland system, though not to the full degree as restrictions we see on the mainland.

a) Arrests and attacks on journalists

Several incidents in the past year demonstrate that Hong Kong authorities are prepared to use criminal penalties against Hong Kong journalists, including labeling newspaper articles as a threat to national security, in order to muzzle critical coverage of police misconduct or government policies. The use of NSL criminal charges against staff of the *Apple Daily* newspaper led to its closure in June 2021. Other journalists have faced charges ranging from obstructing police, resisting arrest, or making false statements for accessing public information.[19]

The targeting of the press stems in part from the 2019 protests, during which journalists from a range of publications as well as student journalists and freelancers, reported critically on police misconduct and the government response to protesters. Numerous incidents of police brutality were documented by journalists and shared around the world. The level of press scrutiny on the protests was widespread compared to the coverage of dissent in mainland China and was an example of the relative openness of Hong Kong's system. That system is now under threat.

Media personalities have faced arrest for content critical of the Chinese and Hong Kong governments, with the NSL's new standards on due process rights extending beyond NSL charges. In February 2021, Hong Kong national security officers arrested radio host Wan Yiu-sing for "committing an act with seditious intent" under the colonial-era Crimes Ordinance over comments that he made on his shows the previous year.[20] He remains in custody awaiting trial under the new standard against the presumption of bail created by Article 42 of the NSL because his case "involved behavior endangering national security."[21]

Authorities have threatened media with prosecution under the NSL for their coverage of the government. Hong Kong's police commissioner and senior ministers threatened local media over their coverage of an event promoting the NSL in April 2021. The commissioner said that police could investigate or arrest individuals for "fake news" under the NSL.[22]

Journalists also face prosecution on non-NSL charges for investigative reporting. In one prominent example, freelance producer Bao Choy was convicted in April 2021 of making "false statements" and fined HK$6,000 (US$770) for accessing a government database for a documentary produced for public broadcaster Radio Television Hong Kong (RTHK) about the July 2019 Yuen Long mob attack.[23] The US State Department denounced her arrest and journalist associations decried it as an attack on press freedom.[24] The politicized nature of her conviction was reflected when prosecutors dropped charges against a state media journalist in June 2021 after they had been arrested on the same charge.[25]

Another recent development in Hong Kong has been an uptick in physical attacks on individual journalists and the printing press of the *Epoch Times* newspaper. The newspaper, which was founded by practitioners of the Falun Gong spiritual movement, often covers human rights abuses in China and is fiercely critical of the CCP. Between April-May 2021, unidentified men attacked the *Epoch Times* printing press with sledgehammers and assaulted a journalist with a bat outside her home.[26] This was the second attack on the newspaper's printing press since 2019 and the fifth in 15 years. In March, another Hong Kong-based *Epoch Times* journalist reportedly

received threats from mainland police, who detained and questioned her mainland-based family members.[27] Falun Gong is banned and its practitioners severely persecuted on the mainland for practicing their faith or sharing information about it, but they are currently still allowed to meditate in public and disseminate leaflets in Hong Kong. Nevertheless, the Secretary for Security Chris Tang said in July that police would investigate whether the group had violated the NSL.[28]

b) The Silencing of Apple Daily

The crackdown and closure of *Apple Daily* is emblematic of how the NSL is being used to stifle press freedom. It is reflective of the CCP's tactic to target key individuals in order to send a warning signal to others of the risks of speaking out and challenging the party's authoritarian rule. The crackdown on *Apple Daily* also reinforced the retroactive nature of the NSL.

The paper, founded in 1995 and with a strong prodemocracy editorial line, was one of Hong Kong's largest newspapers. It's owner, Jimmy Lai, was the first from the media sector targeted by police with the NSL. In August 2020, police arrested Lai on suspicion of "colluding with foreign powers" and raided the newspaper's office.[29] At the center of the NSL charges against Lai are public calls, including in media interviews and from his Twitter account, for foreign governments to impose sanctions on Hong Kong and Chinese officials responsible for violating rights and freedoms in Hong Kong—actions the US government has taken.[30] Lai was denied bail in a landmark ruling from the Court of Final Appeal.[31] After his arrest, a network of 40 convenience stores owned by a company with strong business ties to mainland China announced that it would stop selling *Apple Daily*, demonstrating some of the economic pressure on opposition media from pro-Beijing forces.[32] Then in May 2021, police froze Lai's HK$500 million (US$64 million) worth of assets and shares in the paper's parent company and three other companies using powers under the NSL.[33]

As *Apple Daily* continued to critically cover news events despite Lai's jailing, authorities turned their sights on the paper itself, leading to its closure. *Apple Daily* released its final edition on June 24, 2021 and shut down its website, online television channels, and social media accounts following an unprecedented police raid and the arrests of its chief editor, other newsroom staff, and executives at the parent company Next Digital, all under the NSL.

Authorities accused the newspaper's staff of "colluding with foreign forces" by publishing articles—beginning in 2019, prior to the NSL's adoption—that called for foreign sanctions against Hong Kong and Chinese government officials. Police also arrested on charges of "conspiracy to collude with foreign forces" the paper's lead opinion writer and a former editorial writer at the airport.[34] Police froze HK$18 million (US$2.3 million) in corporate assets, leaving Next Digital unable to pay staff or receive payments from lenders.[35] As a result of the financial and legal risks, the company closed *Apple Daily*, a sister publication, *Next Magazine*, and on July 1 the publicly-traded company ceased operations.[36]

The crackdown on *Apple Daily* sparked fear among other independent outlets, like Stand News, which removed its online commentary articles and took measures to protect staff.[37] Another

independent media outlet, Initium News, announced in August it was relocating to Singapore, though Hong Kong staff are not required to move.[38]

c) Transformation of public broadcaster RTHK into state media

The government takeover of Radio Television Hong Kong (RTHK) has been a swift transformation of a once respected public broadcaster, and one of the changes under the NSL that will be most felt widely in Hong Kong. RTHK, founded in 1928 and modelled after the British Broadcasting Corporation (BBC), had been a widely respected and award-winning source of news and diverse viewpoints in Hong Kong in Cantonese, English, and Mandarin. Its charter ostensibly guaranteed its editorial independence, though as a government department, its independence ultimately depended upon the government to respect that distinction. The takeover of RTHK started in the aftermath of the prodemocracy protests, when RTHK's reporting came under attack from pro-Beijing groups as being "biased," and the government ordered a review of RTHK's management and activities in response.

In February 2021, RTHK lost its editorial independence when the Hong Kong's government appointed bureaucrat Patrick Li with no broadcasting experience to head the broadcaster, just ahead of the publication of a government report that said RTHK lacked "clear editorial accountability."[39] Other government bureaucrats soon joined Li on the management team and several RTHK journalists and executives resigned or were fired.[40] Li announced an unprecedented policy—that all programs going forward would need to be reviewed and approved personally by him, which led to several shows and programs being censored. RTHK also announced staff could be held financially liable for censored programs, and threatened fines against reporters in May 2021 for airing a video of a previous Tiananmen vigil without authorization.[41] In April 2021, RTHK launched a new show hosted by Hong Kong chief executive Carrie Lam—to be aired four times a day. In August, RTHK further turned into a propaganda outlet when Carrie Lam announced that RTHK will partner with Chinese state media giant China Media Group to broadcast programming to "nurture a stronger sense of patriotism."[42]

d) Ownership of media and presence of state or mainland-linked actors

Hong Kong media is suffering from a multitude of challenges beyond political and legal scrutiny. The Chinese state owns several newspapers, which while traditionally have ranked low in terms of public trust but are increasingly being used by authorities to guide crackdowns and target individual activists and civil society organizations. Private media also faces financial stress which can led to takeover by mainland-linked actors who shift or ensure pro-Beijing editorial lines.

Currently there are two newspapers in Hong Kong directly owned by the Chinese state through the Liaison Office of the Central Government in the Hong Kong Special Administrative Region: *Ta Kung Pao* and *Wen Wei Po*. In 2016, the two papers merged editorial and technical departments but still publish as separate papers.[43] They rank low on credibility in public opinion polls and have low levels of readership, but the papers have taken to issuing editorials attacking opposition and prodemocracy figures which are later targeted by the police, and exemplify the

type of state media smears used in the mainland. For example, in April 2021, *Ta Kung Pao* called for *Apple Daily* to be banned for "endangering national security" prior to the raids on the paper,[44] and recently *Wen Wei Po* attacked the Hong Kong Journalist Association as "anti-government."[45]

In February 2021, Hong Kong's oldest Chinese-language newspaper, *Sing Tao*, was purchased by the daughter of a Shenzhen-based property tycoon.[46] Following the acquisition, in August, the US Department of Justice ordered the paper's US subsidiary to register as a foreign agent under the Foreign Agents Registration Act (FARA).[47] In April 2021, pro-Beijing Phoenix Television founder Liu Changle sold his stake in the broadcaster to Chinese state-owned Bauhinia Culture Holdings and the Hong Kong-Macau company Shen Tuk Holdings, making the majority of Phoenix TV state-owned.[48] Three new directors were brought in, all of whom are believed to have previously worked for the central government in Beijing.[49] Phoenix TV broadcasts in the United States and due to the ownership changes, should also be required to register under FARA.

Recent regulatory moves in the mainland have implications for the media environment in Hong Kong. Alibaba-owned *South China Morning Post*, Hong Kong's oldest English-language newspaper, is facing the prospect of new ownership after mainland regulators reportedly ordered Alibaba to divest its media holdings.[50] There are fears that the paper could be bought by a Chinese state-owned company or mainland billionaire who would dramatically transform the paper's editorial line and coverage. Jack Ma's ownership of the paper, while criticized at times, has generally continued to allow independent reporting by its journalists – especially during its coverage of the 2019 protests but even up to the present – although editorials and some opinion articles published tend to favor Beijing's line more closely than before.

Economic pressure on media is present in the Hong Kong market as well as around the world. For example, in December 2020, iCable TV, a once well-respected private media company, laid off 40 workers from its award-winning investigative news program *News Lancet* ostensibly due to financial pressure caused by the COVID-19 pandemic.[51] The program was known for its coverage of politically sensitive stories, and numerous other journalists resigned in protest at the sudden decision.[52] *Apple Daily* used to employ 1,000 people and many reporters found themselves unemployed due to the paper's closure. Some expressed fear about finding a new job in Hong Kong's media environment due to their previous employer.[53] While some independent digital news outlets like Hong Kong Free Press and Citizen News rely on an innovative business model of public donations, those methods could be targeted by the government. Police have arrested other prodemocracy figures on accusations of "money laundering" for crowdfunding.[54]

e) Administrative measures to restrict press freedom

Several administrative changes brought in by Hong Kong police and government bodies have infringed on press freedom by preventing journalists from accessing public records, a common tool of investigative journalists, or preventing journalists from working freely in the territory. Coupled with the conviction of journalist Bao Choy for accessing a public database, the changes send a chilling signal to the press. While the government has claimed some of these measures are to protect "privacy," there is no allowance for accessing information for the public interest and the actions appear to target public records previously used to expose official corruption or

wrongdoing. Hong Kong's famously muckraking media sector was well-known for combing through records to expose official's transgressions, such as exposing in 2018 that Secretary of Justice Teresa Cheung had illegal structures at her home.[55]

The changes to government records include March 2021 amendments to restrict access to information about directors of companies on the Hong Kong's Companies' Registry.[56] In May, the passage of the Improving Electoral System Bill 2021 restricted access to electoral roll information.[57] Authorities have also restricted access to birth and marriage records and vehicle transport records, the same system which journalist Bao Choy used.[58]

Police announced in September 2020 that the designation of "media representative" would be limited to government-registered and "well-known" international agencies, an attempt to replace a system that was based on membership in journalist unions.[59] In July-August 2020, immigration authorities refused to issue visas to a *New York Times* correspondent and to an editor of the Hong Kong Free Press.[60] The *Times* announced that it would move its Hong Kong–based digital news operations to South Korea, demonstrating some of the challenges facing American media in the territory.[61] The Foreign Correspondents' Club of Hong Kong described a highly unusual number of visa delays for journalists in Hong Kong in 2020.[62] Denial of journalist visas is a common CCP tactic and has been particularly used against US journalists and US media organizations on the mainland. If Hong Kong authorities were to start to increasingly deny visas or registration of Hong Kong journalists in the government system to exclude critical journalists, press freedom would worsen further. The quality of news and information available to US businesses and investors would also be more severely impacted.

2) Internet freedom trends under the National Security Law

Hong Kong has traditionally enjoyed a free and open internet, one of the reasons many foreign media and businesses made the territory its base in Asia. Specific provisions under the NSL place that free internet at risk, especially for platforms or content critical of the government. Under Article 43 of the NSL and the implementing measures enacted by the Hong Kong government, police are empowered to order the blocking and deletion of content by message publishers, platform service providers, hosting service providers, and/or network service providers. Police can also intercept communications or conduct covert surveillance under approval of the Chief Executive.[63] Those who do not comply with these provisions, including technology firm employees, could face fines or even prison sentences.

a) Blocking websites

One of the most prominent features of the mainland Chinese internet is the blocking of certain websites. In January 2021, Hong Kong authorities blocked access to a website for the first time, justifying the move under the NSL. The blocked site, HKChronicles, is a platform that has been used by activists to dox police officers (among them, those involved in attacking protesters) and expose pro-Beijing businesses.[64] Afterwards, four websites, all with Taiwan-based IP addresses, were blocked, though two sites became accessible after three days. Some had clear links to the protest movement, such as the site of a Taiwanese church that raised donations for Hong Kong protesters, but the others were websites of Taiwan's ruling party, a military recruitment platform,

and the transitional justice commission. Then in June, Hong Kong internet service providers blocked access to the exile website 2021 Hong Kong Charter (2021hkcharter.com).[65] Earlier that month, the website temporarily went down globally after Hong Kong police ordered its Israel-based hosting provider to close it.[66] This was the first instance of Hong Kong authorities invoking the extraterritorial jurisdiction of the NSL against a website.

b) Content removal/censorship

The majority of content removal has come through self-censorship, though police have flexed their powers to demand the removal of internet content. Content removal has been a significant consequence of the attacks on independent and prodemocracy media. All of *Apple Daily's* online content has been removed, a loss which will be felt in Hong Kong and globally. It had 600,000 paid subscribers at the time of its closure, and its website received nearly 18.7 million visits in May. The newspaper had 2.6 million Facebook followers, 1.89 million followers on its YouTube channel, 1 million followers on its Instagram account, and over 500,000 followers on Twitter. The deletion of all of these accounts cut off audiences and was a monumental loss of millions of articles and social media posts.[67] A group of individuals launched a crowdsourced effort to help scrap some of the website before it closed and saved two million pages and put them on the website collection.news.[68]

In June, Stand News removed all of its online opinion articles following the arrests of *Apple Daily* staff.[69] RTHK was a major source of high-quality Cantonese-language content, but under government management the broadcaster deleted all its content older than one year from Facebook and YouTube and removed all of its posts from its English-language Twitter account, which often wryly mocked government actions.[70] Hong Kong netizens have tried to archive past programs on a blockchain platform before they were taken down.[71]

Compared to website blocks, whereby the censored content remains online and accessible outside of the territory, such large-scale content removals have effectively erased decades of independent reporting and commentary not only for users in Hong Kong but globally.

In 2019, Apple removed an app from its app store that was used to track police movements during the protests under pressure from the government. Google removed a separate app related to the protests for violating its policy of "capitalizing on sensitive events."[72] Facebook has removed several popular pages run by prodemocracy and pro-police groups without explanation.[73] Most major foreign technology companies, including American companies, announced they would not comply with government requests for user data in the aftermath of the NSL, though the companies' transparency around government takedown requests could be stronger.[74]

c) Arrests for online activity

Some of the examples provided in this testimony are of individuals arrested because of their online expression or activities. Arrests and prosecutions for online activity have become more common in Hong Kong, a practice that is routine in the mainland under the CCP. In April 2021, a Hong Kong court sentenced the administrator of a Telegram channel with approximately

60,000 subscribers that was used during the 2019 protests to three years in prison for "conspiracy to commit a seditious act" and "conspiracy to incite others to commit arson" over the comments shared in the channel.[75]

New and proposed legislation will further restrict free expression online and creating a chilling effect in Hong Kong. These include a bill to extend the Beijing-imposed ban on "desecrating" the Chinese flag or emblems to include acts online.[76] A new electoral law passed in May 2021 criminalized inciting someone to spoil or leave blank their ballot, which could lead to arrests for online campaigning in December 2021's Legislative Council elections. In July, the government introduced a bill banning doxing which may lead to further arrests for online activity.

d) Surveillance of opposition figures

The NSL authorized expanded covert surveillance of individuals accused of endangering national security. The expansion of surveillance, including intercepted communications, puts prodemocracy activists and participants of the 2019 protests at serious risk of arrest and prosecution. Mass and targeted surveillance is a feature of the mainland system and in addition to violating an individual's right to privacy, has severe psychological repercussions. This is exemplified in the tragic case of mainland dissident Li Huizhi who took his own life in July 2021 and cited police surveillance as making his life unbearable.[77]

While government surveillance is hard verify there are indications in Hong Kong of government hacking or tracing of online activity of prodemocracy activists. In December 2019, activist Joshua Wong claimed Hong Kong police had hacked into his phone after arresting him and seizing his device in August, as they submitted text messages as evidence in his trial.[78] In another earlier incident, in June 2019, police arrested the administrator of a 30,000 member protest-related Telegram channel from his home (rather than a protest site) on charges of "conspiracy to cause a public nuisance." They forced him to unlock his phone and export a list of the group's members.[79]

e) Cyberattacks:

There have been numerous cyberattacks linked to the Chinese state, originating in China, or from unidentified actors on websites and platforms used by protesters and civil society in Hong Kong. Telegram and LIHKG.com, used by protesters to organize and communicate online, suffered large distributed denial-of-service (DDoS) attacks during the 2019 protests.[80] The Amnesty International Hong Kong office, local universities, and Android and iOS users in Hong Kong were targeted by malware.[81] Many of these attacks were an attempt to censor prodemocracy activists and have implications for American businesses or individuals in Hong Kong who use such platforms or may be targeted by a cyberattack if they cross the government.

3) How Hong Kong's media and internet space is still different from Mainland China

Beijing's transformation of Hong Kong, while swift and dramatic, has not fully changed the territory into a mainland city. While human rights and freedoms in Hong Kong have eroded, there remains some important distinctions compared to the mainland system. These distinctions

are important to acknowledge to show how the systems continue to be different but also as areas to watch and protect from further restrictions.

1) **Reporters are still publishing independent coverage of news events**. There are still independent journalists reporting in Hong Kong without government interference unlike in the mainland. Reporters, while restricted and increasingly the focus of arrests, are by and large still allowed to question government officials, attend press conferences, and operate freely in the city. The level of government management of accredited journalists is not subject to the same level of interference as in the mainland, where reporters must pass a test on "Xi Jinping Thought" and have their social media posts combed through.[82] Many of the sources cited in this testimony come from reporters and media based in Hong Kong, albeit the *Apple Daily* links no longer work.

2) **Independent media is allowed to exist.** While ownership and economic pressures on journalists are great, private, independent media exists in Hong Kong, such as Stand News, Hong Kong Free Press, Citizen News, inmediahk, and *Epoch Times* who regularly publish content that is critical of the Hong Kong government or covers sensitive issues that private media in China is not allowed to. There are no propaganda directives to media to cover issues in a certain way or only use state media copy, as is found on the mainland.[83] While the *New York Times* moved their Hong Kong bureau, they continue to have reporters in Hong Kong and other foreign and American media operates in the territory without being subject to the same government restrictions as their mainland counterparts. Though the media regulator in Hong Kong, the Communications Authority, has issued penalties for political or news commentary that pro-Beijing forces complained about, it has to date not suspended the license of any independent media outlet.

3) **Websites are by and large not blocked.** While website blocking has increased under the NSL, to date only six websites have been blocked. This is vastly different from the mainland system where the Great Firewall currently blocks thousands of websites. Facebook, Twitter, and other international websites not only continue to be accessible in Hong Kong they are still some of the dominant platforms used by Hong Kongers. No media websites have been blocked, to date.

4) **Self-censorship vs censorship**. While there have been numerous incidents of content removal, they have largely been taken down by the publisher of the content without a legal request. While the NSL permits police to order content to be removed, such powers have not yet been exercised in as widespread manner as in the mainland. Much of the deleting of posts on social media in the mainland is done by departments in private PRC-based technology companies, such as Tencent's WeChat and Sina Weibo. American technology companies should ensure that they do not remove content on the orders of the Hong Kong police or because the content is politically sensitive to the CCP.

4) Long-term forecasts on the media and internet space

As this analysis has covered, an emboldened Beijing has demonstrated it will continue to crackdown on Hong Kong until there is no opposition left. There are several areas to watch for

further shrinking of space for press and internet freedom in Hong Kong. The US government and interested groups should proactively prepare for further crackdowns in Hong Kong and be ready for when they come with a range of tools.

1. **Legislation to further clamp down on a free press**. Chief Executive Carrie Lam announced on May 4, 2021 that the government was working on "fake news" legislation.[84] Pro-Beijing politicians supported the move and called for the government to legislate against content that "incites hatred of the government."[85] In May, the digital news site Post 852 announced it was suspending operations, with the founder acknowledging the outlet's financial struggles but pointing to the expected "fake news" law as the primary catalyst for the decision. He consequently dismissed the outlet's entire staff.[86] A "fake news" law will have serious ramifications for press freedom, including potential closures of media organizations, lawsuits and criminal prosecution of journalists and news outlets, as well as further self-censorship and content removal.

2. **Legislation which could usher in government censorship online.** In July, the government introduced the Personal Data (Privacy) (Amendment) Bill to outlaw doxing.[87] It would permit employees of overseas technology companies to be arrested and jailed for two years if the companies fail to comply with takedown requests.[88] The Hong Kong privacy commissioner would also be empowered to conduct warrantless searches. The Asia Internet Coalition, an industry body that counts American companies like Google, Twitter, and Facebook as members, sent a letter to the Privacy Commissioner and denounced some of the amendments as "unnecessary and excessive."[89] It highlighted that the only way for companies to avoid the sanctions under this bill would be to avoid doing business in Hong Kong. The Legislative Council, which has no opposition members, has begun debating the bill and it will likely be voted into law soon.[90] American companies may find that they are forced to choose between complying with censorship requests, having their employees jailed in a standoff, or in the long-term quitting the Hong Kong market, leaving it open to being dominated by compliant mainland companies. They should consider how they might attempt to challenge takedown requests that violate the Basic Law in Hong Kong courts.

3. **Forced sale or government pressure to close independent media**. *The South China Morning Post*, sometimes called Hong Kong's paper of record, faces the prospect of a sale to a Chinese state entity or individual and being turned into a propaganda outlet. Other smaller, especially Chinese-language, independent media may be forced to relocate or close in order to maintain their independent coverage, as witnessed with the relocation of Initium Media to Singapore. It is likely that journalists may continue to be arrested if they critically cover events and that self-censorship grows.

4. **Eroding legal protections for the press**. In April 2021, *Apple Daily* reported that the Justice Department ruled that searches of journalistic material in national security investigations could be conducted without court approval, as existing legislative oversight rules did not extend to the Beijing-imposed NSL.[91] During the June 2021 raid on the paper, police seized journalist materials and searched through the newsroom. In August, police deployed the NSL to demand that a civil society group hand over any materials pertaining to contact with "foreign forces," which experts decried was a fishing expedition and could infringe on their

due process rights.[92] Increased use of warrantless searches against media organizations could endanger sources and put reporters at risk of prosecution. Arrested individuals in Hong Kong are allowed to retain independent lawyers of their own choice, unlike in the mainland following the drastic 2015 crackdown on human rights lawyers. Nevertheless, due process rights have been eroded with the new widespread denial of bail in national security cases. Further features of the mainland legal system may be brought to Hong Kong.

5. **Asset seizures under the NSL**. The closure of *Apple Daily* and its parent company Next Digital after police froze Jimmy Lai's shares and the company's assets demonstrate the sweeping ways the NSL can be used against businesses. Following Next Digital's closure, the Hong Kong government announced it had appointed a special fraud investigator for the first time since 1999 to investigate whether the company had committed fraud by using the company to "conduct unlawful activities."[93] The CCP essentially stripped a businessman of his assets and closed his company because of his political views, actions that should make every business operating in the territory take note. With the NSL and the likelihood of China's Anti-Sanctions Law being imposed on Hong Kong, businesses could be faced with financial losses, police investigations, or sanctions if they remain in Hong Kong.[94]

6. **Regional and global impact on Chinese-language media**. *Apple Daily*'s parent company Next Digital announced on July 29 it had sold its Taiwanese arm, which included *Apple Daily Taiwan* which continues to publish online though not in print.[95] Two days later the company ceased operations. The sale of *Apple Daily Taiwan*, to an undisclosed party, and the previous financial pressure that caused Next Digital to cease printing the Taiwanese edition in April 2021 demonstrates the regional and global implications of the crackdown on the free press in Hong Kong.[96] Independent, credible news in the Chinese-speaking region traditionally included Hong Kong's press and further crackdowns will be felt beyond Hong Kong's borders and amongst the Chinese and Hong Kong diaspora communities, including in the United States.

7. **Further violations of international agreements and treaties**. The speed with which the CCP violated the Sino-British Joint Declaration, the Basic Law, and the International Covenant on Civil and Political Rights in Hong Kong demonstrates its lack of sincerity towards its international commitments. The CCP's lack of respect for its international legal obligations has ramifications for business operating in Hong Kong and governments signing treaties or agreements with the CCP on a range of issues like trade and climate change.

Recommendations

Hong Kongers are now living in a high risk territory where they could face potential life in prison for exercising their human rights. Moreover, the impact of the crackdown on media and internet freedom in Hong Kong is being felt far beyond the territory's borders, including here in the United States. Despite the rapidly deteriorating situation and Beijing's seeming intransigence to international pressure, there are steps that the US government can take to:

1) Help journalists, media owners, and activists fleeing Hong Kong to the United States

- The Biden Administration should use **humanitarian parole for Hong Kongers**, while bringing US refugee resettlement numbers back to historical levels. Congress should provide adequate funding for this purpose**.**

- **Congress should pass legislation**, either as a standalone measure or as part of a larger bill, **to ease and hasten entry into the US** for Hong Kongers being targeted for their peaceful involvement in human rights activities. This could include the Hong Kong People's Freedom and Choice Act, which enjoys bipartisan support and would, among other things, provide temporary refuge to Hong Kongers already in the US who face persecution if forced to return, and expedite the processing of refugee applications for Hong Kongers at risk.

- The State Department should **respond forcefully** to any reported attempts by Chinese diplomats or security services to intimidate, harass, or attack Hong Kong journalists and online activists in the United States.

- The US government should **support independent Chinese-language media, including in Cantonese.** To the extent that it is safe to do so and there is an interest on the part of journalists fleeing Hong Kong, the US government and other media development funders should ensure that exile Hong Kong and diaspora outlets are included in projects that offer funding, training, and other assistance opportunities. Funders should provide technical and financial support to strengthen cybersecurity among independent Chinese-language and Hong Kong-oriented outlets.

2) Take action to protect journalists and internet users remaining in Hong Kong

- **Continue to publicly condemn attacks on press and internet freedom in Hong Kong.** Members of Congress and the Biden Administration have done well to issue statements of concern or condemnation on individual cases or incidents involving attacks on press and internet freedom, including Bao Choy's conviction and the police raids on *Apple Daily*. They should continue to exert public and private pressure on Chinese and Hong Kong officials, including calling for the release or dropping of charges against individual journalists or activists, such as currently detained journalist-turned politician Gwyneth Ho and the *Apple Daily* executives and news staff.

- **Use digital security best practices** for any communications with or about Hong Kong-based journalists and advocates. Given the sweeping powers under the NSL to conduct covert surveillance and police practice used on the mainland to persecute individuals for contact with overseas individuals or entities, any communications regarding Hong Kong activists or with those individuals should be done with extraordinary caution and digital security best practices.

- **Encourage American technology companies to resist state demands that violate users' rights,** including by rebuffing requests for user data or to remove, block, or otherwise censor content that is protected under international human rights standards. Encourage companies to be fully transparent around government requests or their own removal of content, whether or not companies comply, which would lay bare the state's repressive actions.

- **Encourage American technology companies to divert internal resources to protect internet freedom in Hong Kong** in preparation for the potential onslaught of attacks likely in the coming months. Social media companies should roll out security features to protect users from state-sponsored hackers and increase staff capacity to rapidly respond to incidents, including account takeovers and reports of disinformation or harassment. VPN providers can bolster resources to evade blocks on websites and circumvention tools. Website hosting providers can expand distributed denial-of-service (DDoS) mitigation services for independent media and civil society facing state-sponsored cyberattacks. Companies can also help protect the privacy and safety of users – and improve their own preparedness – by proactively engaging with and providing support to civil society groups working on digital rights and safety.

- **Congress should hold hearings or private briefings** and meetings with private US companies on the evolving conditions in Hong Kong, particularly as they pertain to US companies' operations in the territory potentially being used to infringe on media and internet freedom.

3) Enforce US laws to reflect changing Hong Kong media ownership

Mainland-linked companies, entrepreneurs, and state-owned enterprises have begun purchasing or investing in media outlets in Hong Kong who also broadcast or print through US subsidiaries. US government enforcement of relevant laws, including the Foreign Agents Registration Act (FARA), should keep pace.

- Due to the **change in ownership at Phoenix Television**, the Department of Justice should order the company to register under FARA and submit the necessary disclosures, similar to recent action related to *Sing Tao*. Phoenix TV is widely available throughout the United States and relatively popular among Chinese speaking viewers. Congress should ensure that the department has sufficient staff and resources to evaluate and monitor the shifting media landscape in Hong Kong, including any future sale of the *South China Morning Post,* and its implications for the US media market.

4) Use international human rights mechanisms to pressure the Hong Kong and Beijing governments.

The Chinese and Hong Kong governments have violated their obligations under international law to protect the rights guaranteed to Hong Kongers under the International Covenant on Civil and Political Rights, which had been ratified in the territory (contrary to mainland China, where the treaty was only signed but never ratified) and enshrined in the Basic Law.

- The United States should call on the UN High Commissioner for Human Rights or a relevant UN human rights expert, like the Special Rapporteur on Freedom of Expression, the Working Group on Arbitrary Detention, or the Special Rapporteur on Torture to **request a visit to Hong Kong** to visit political prisoners and assess the situation on the ground for jailed journalists, media owners, and human rights defenders.

- The United States should proactive engage with allies and raise cases and media and internet freedom issues at the **UN Human Rights Council** through oral statements, high-level side events, and engagement with civil society organizations.

[1] "Xi Focus: Xi stresses "patriots governing Hong Kong" when hearing Carrie Lam's work report," Xinhua News Agency, January 27, 2021, http://www.xinhuanet.com/english/2021-01/27/c_139702049.htm
[2] Freedom House, Election Watch for the Digital Age – Hong Kong, (accessing August 27, 2021) https://freedomhouse.org/report/election-watch-digital-age#hong-kong
[3] Jessie Yeung and Chermaine Lee, "First person charged under Hong Kong's national security law sentenced to 9 years in prison," CNN, July 30, 2021 https://www.cnn.com/2021/07/30/asia/tong-ying-kit-hong-kong-sentencing-intl-hnk/index.html
[4] "Tony Chung: Hong Kong activist detained near US consulate charged," British Broadcasting Corporation (BBC), October 29, 2020 https://www.bbc.com/news/world-asia-china-54729054
[5] Austin Ramzy and Tiffany May, "The Latest Target of Hong Kong's Crackdown: Children's Books," The New York Times, July 30, 2021 https://www.nytimes.com/2021/07/22/world/asia/hong-kong-children-book-arrests.html
[6] Zen Soo, "Hong Kong bans Tiananmen crackdown vigil for 2nd year," Associated Press (AP), May 21, 2012 https://apnews.com/article/hong-kong-health-coronavirus-pandemic-bfe4f7f1fd301dbad4d8c4906c1c73b3; Tony Cheung , Chris Lau and Christy Leung, "Hong Kong police deny groups' application for July 1 rally against 'political suppression'," South China Morning Post (SCMP), June 28, 2021 https://www.scmp.com/news/hong-kong/politics/article/3139022/hong-kong-police-deny-groups-application-july-1-rally; Natalie Wong, "Hong Kong national security law: police ban July 1 march planned to protest against legislation," SCMP, June 27, 2020 https://www.scmp.com/news/hong-kong/politics/article/3090848/hong-kong-national-security-law-police-ban-july-1-march.
[7] Hong Kong Police, "5 Key Figures • Telling Right from Wrong [五大數據 • 明辨錯對]", May 14, 2020, https://www.facebook.com/HongKongPoliceForce/photos/a.965784490176182/3176913899063219/
[8] Stand News, "In the past 3 years, 7 workers' unions disband "過去 3 年 7 職工會自行解)," August 25, 2021 https://www.thestandnews.com/politics/%E9%81%8E%E5%8E%BB-3-%E5%B9%B4-7-%E8%81%B7%E5%B7%A5%E6%9C%83%E8%87%AA%E8%A1%8C%E8%A7%A3%E6%95%A3-%E7%BE%85%E8%87%B4%E5%85%89%E8%8B%A5%E6%9B%BE%E9%81%95%E6%B3%95%E5%AE%9A%E5%BF%85%E5%9A%B4%E8%82%85%E8%B7%9F%E9%80%B2
[9] Jessie Yeung, "Prominent Hong Kong civil rights group disbands, citing government pressure," CNN, August 15, 2021 https://www.cnn.com/2021/08/15/asia/hong-kong-chrf-disbands-intl-hnk/index.html
[10] "Largest Hong Kong teachers' union disbands amid government crackdown," AP, August 10, 2021, https://www.cnbc.com/2021/08/11/largest-hong-kong-teachers-union-disbands-amid-government-crackdown.html; Sarah Cheng, "Hong Kong's Lam tells solicitors' group to stay out of politics," Reuters, August 17, 2021 https://www.reuters.com/world/asia-pacific/hong-kong-leader-says-no-explicit-timetable-anti-foreign-sanctions-law-2021-08-17/
[11] Chan Ho-him, "Hong Kong experiences 'alarming' population drop, but government says not all 90,000 leaving city because of national security law," SCMP, August 12, 2021 https://www.scmp.com/news/hong-kong/society/article/3144845/hong-kongs-experiences-alarming-population-drop-government; Jamie Grierson, "UK receives 34,000 visa requests from Hong Kong in two months," Guardian, May 27, 2021 https://www.theguardian.com/world/2021/may/27/uk-receives-34000-visa-requests-from-hong-kong-in-two-months

[12] Steve Vines, "Loving Hong Kong has become a suspect activity – why, at last, it was time to leave," Hong Kong Free Press (HKFP), August 6, 2021 https://hongkongfp.com/2021/08/06/steve-vines-loving-hong-kong-has-become-a-suspect-activity-why-at-last-it-was-time-to-leave/
[13] "Hong Kong passes immigration bill, raising alarm over 'exit bans'," Reuters, April 27, 2021 https://www.reuters.com/world/asia-pacific/hong-kong-passes-immigration-bill-raising-alarm-over-exit-bans-2021-04-28/
[14] Selina Cheng, "Hong Kong national security police bar reporter who filmed police stabbing from leaving city, home searched," HKFP, July 27, 2021 https://hongkongfp.com/2021/07/27/hong-kong-national-security-police-bar-reporter-who-filmed-police-stabbing-from-leaving-city-home-searched/
[15] Sarah Cook, "Red Flags for Free Expression in Hong Kong," Freedom House, June 2020 https://freedomhouse.org/report/china-media-bulletin/2020/hong-kong-warning-signs-us-protest-coverage-citizen-defiance-june#A1
[16] Fion Li and Vinicy Chan, "Security Law Sends Hong Kong Residents Dashing for the Exit," Bloomberg, May 30, 2020 https://www.bloomberg.com/news/articles/2020-05-31/china-s-security-law-sends-hong-kong-residents-dashing-for-exit
[17] Hong Kong Journalist Association (HKJA), "2021 Annual Report: Freedom in Tatters," July 15, 2021 https://www.hkja.org.hk/en/%e6%9c%aa%e5%88%86%e9%a1%9e-en/2021-annual-report-freedom-in-tatters/
[18] HKJA, "Hong Kong Press Freedom Index for journalists hits record low HKSAR blamed as Hong Kong's press freedom plunges to worst record," May 3, 2021 https://www.hkja.org.hk/en/press-freedom-index/hong-kong-press-freedom-index-for-journalists-hits-record-low-hksar-blamed-as-hong-kongs-press-freedom-plunges-to-worst-record/
[19] Kelly Ho, "Student journalist charged with obstructing Hong Kong police and resisting arrest during mall demo," HKFP, November 4, 2020 https://hongkongfp.com/2020/11/04/student-journalist-charged-with-allegedly-obstructing-hong-kong-police-and-resisting-arrest-during-mall-demo/; Rhoda Kwan, "Hong Kong police arrest journalist for 'obstruction' after she filmed arrests," HKFP, November 6, 2020 https://hongkongfp.com/2020/11/06/hong-kong-police-arrest-journalist-for-obstruction-after-she-filmed-arrests/
[20] Committee to Protect Journalists, "Hong Kong police arrest internet radio host Wan Yiu-sing on sedition charges," February 8, 2021 https://cpj.org/2021/02/hong-kong-police-arrest-internet-radio-host-wan-yiu-sing-on-sedition-charges/
[21] Kelly Ho, 'Hong Kong radio host 'Giggs' denied bail ahead of trial for allegedly 'seditious' broadcast," HKFP, February 10, 2021 https://hongkongfp.com/2021/02/10/hong-kong-radio-host-giggs-denied-bail-ahead-of-trial-for-allegedly-seditious-broadcast/
[22] Victor Ting, "Hong Kong police, security chief issue 'fake news' warnings over media coverage of national security events," SCMP, August 16, 2021 https://www.scmp.com/news/hong-kong/politics/article/3129829/hong-kong-police-security-chief-issue-fake-news-warnings
[23] Reporters without Borders, "Hong Kong: investigative journalist Bao Choy convicted of "false statements," April 23, 2021 https://rsf.org/en/news/hong-kong-investigative-journalist-bao-choy-convicted-false-statements
[24] Jalina Porter @StateDeputySpox "The U.S. is deeply concerned about the arrest of Hong Kong journalist @baochoy on charges related to her work as an investigative journalist. The Chinese Communist Party and their Hong Kong proxies must cease efforts to crush press freedom." November 4, 2020 https://twitter.com/StateDeputySpox/status/1323998950462992389 ; Committee to Protect Journalists, "Hong Kong court convicts, fines journalist Choy Yuk-ling over documentary research," April 22, 2021 https://cpj.org/2021/04/hong-kong-court-convicts-fines-journalist-choy-yuk-ling-over-documentary-research/
[25] Rhoda Kwan, "Charge dropped against Hong Kong state media reporter over improper access to public records, despite RTHK case," HKFP, June 17, 2021 https://hongkongfp.com/2021/06/17/charge-dropped-against-hong-kong-state-media-reporter-over-improper-access-to-public-records-despite-rthk-case/
[26] Freedom House, "China Media Bulletin 153 - April 2021" https://freedomhouse.org/report/china-media-bulletin/2021/retooling-censorship-xinjiang-cotton-hong-kong-press-freedom-april#A5; Freedom House, "China Media Bulletin 154 - May 2021," https://freedomhouse.org/report/china-media-bulletin/2021/gutting-hong-kong-broadcaster-apple-concessions-propaganda#A5
[27] Liang Zhen, "Hong Kong: Reporter and Popular Show Presenter Repeatedly Harassed by CCP," Minghui.org, March 25, 2021 https://en.minghui.org/html/articles/2021/3/25/191568.html

[28] Rhoda Kwan, "Pro-Beijing lawmakers urge gov't to outlaw Falun Gong, target of 3,545 police operations in eight years," HKFP, July 8, 2021 https://hongkongfp.com/2021/07/08/pro-beijing-lawmakers-urge-govt-to-outlaw-falun-gong-target-of-3545-police-operations-in-eight-years/
[29] Committee to Protect Journalists, "Hong Kong police arrest Apple Daily founder Jimmy Lai under new National Security Law," August 9, 2020 https://cpj.org/2020/08/hong-kong-police-arrest-apple-daily-founder-jimmy-lai-under-new-national-security-law/
[30] Selina Cheng, "Pro-democracy media tycoon Jimmy Lai to face new charges under Hong Kong security law," HKFP, December 11, 2020 https://hongkongfp.com/2020/12/11/breaking-pro-democracy-media-tycoon-jimmy-lai-to-face-new-charges-under-hong-kong-security-law/; Al Jazeera, "Jimmy Lai appears in Hong Kong court in metal chain," December 12, 2020 https://www.aljazeera.com/news/2020/12/12/hong-kongs-jimmy-lai-in-court-to-face-national-security-charges
[31] Freedom House, "China Media Bulletin 151 - February 2021," https://freedomhouse.org/report/china-media-bulletin/2021/chinas-information-isolation-new-censorship-rules-transnational#A5
[32] Deutsche Welle, "China Resources' convenience stores stop selling Apple Daily," August 28, 2020 https://www.dw.com/zh/%E5%8D%8E%E6%B6%A6%E6%97%97%E4%B8%8B%E4%BE%BF%E5%88%A9%E5%BA%97%E5%81%9C%E5%94%AE%E8%8B%B9%E6%9E%9C%E6%97%A5%E6%8A%A5/a-54727745
[33] Christy Leung , Phila Siu , Tony Cheung and Ji Siqi, "Hong Kong authorities freeze nearly HK$500 million in assets belonging to media tycoon Jimmy Lai," SCMP, May 14, 2021 https://www.scmp.com/news/hong-kong/law-and-crime/article/3133541/hong-kongs-national-security-police-freeze-nearly
[34] Selina Cheng, "Apple Daily opinion writer arrested by Hong Kong national security police," HKFP, June 23, 2021, https://hongkongfp.com/2021/06/23/breaking-apple-daily-opinion-writer-arrested-by-national-security-police-reports/; Jeffie Lam and Clifford Lo, "National security law: Apple Daily editorial writer arrested at airport while trying to leave Hong Kong," SCMP, June 27, 2021 https://www.scmp.com/news/hong-kong/politics/article/3138957/national-security-law-hong-kong-online-news-portal-pulls
[35] Freedom House, "China Media Bulletin 155 - June 2021," https://freedomhouse.org/report/china-media-bulletin/2021/ccps-insecure-centennial-apple-daily-erased-globalizing-censorship
[36] Candice Chau, "Reddit users race to save Hong Kong Apple Daily content as sections begin to close," HKFP, June 23, 2021 https://hongkongfp.com/2021/06/23/reddit-users-race-to-save-hong-kong-apple-daily-content-as-sections-begin-to-close/; Lilian Cheng, "Hong Kong parent company of Apple Daily to cease operations on Thursday, will still try to pay staff despite authorities not releasing frozen cash," SCMP, June 30, 2021 https://www.scmp.com/news/hong-kong/politics/article/3139345/hong-kong-parent-company-apple-daily-cease-operations
[37] Selina Cheng, "Security law: Stand News opinion articles axed, directors resign amid reported threats to Hong Kong digital outlets," HKFP, June 28, 2021 https://hongkongfp.com/2021/06/28/security-law-stand-news-opinion-articles-axed-directors-resign-amid-reported-threats-to-hong-kong-digital-outlets/
[38] Selina Cheng, "In media first, Hong Kong news outlet Initium quits city for Singapore," HKFP, August 3, 2021 https://hongkongfp.com/2021/08/03/in-media-first-hong-kong-news-outlet-initium-quits-city-for-singapore-over-security-law-fears/
[39] Freedom House, "China Media Bulletin 151 - February 2021"
[40] Freedom House, "China Media Bulletin 152 - March 2021"; Tom Grundy, "Hong Kong journalist who challenged WHO official quits RTHK – sources," HKFP, April 13, 2021 https://hongkongfp.com/2021/04/13/journalist-yvonne-tong-quits-rthk-source/; Selina Cheng, "Hong Kong journalist Steve Vines 'disappointed' to be dropped as commentator from RTHK show," HKFP, April 8, 2021 https://hongkongfp.com/2021/04/08/hong-kong-journalist-steve-vines-disappointed-to-be-dropped-as-commentator-from-rthk-show/; Candice Chau, "Hong Kong's RTHK fires popular pro-democracy radio host Tsang Chi-ho," HKFP, June 19, 2021 https://hongkongfp.com/2021/06/19/hong-kongs-rthk-fires-popular-pro-democracy-radio-host-tsang-chi-ho/
[41] Kelly Ho, "Hong Kong gov't can charge RTHK staff for axed shows, says public broadcaster," HKFP, April 7, 2021 https://hongkongfp.com/2021/04/07/hong-kong-govt-can-charge-rthk-staff-for-axed-shows-says-public-broadcaster/; Amy Nip, "Penalties coming for RTHK staff over June 4 stunt ," The Standard, May 26, 2021 https://www.thestandard.com.hk/section-news/section/11/230591/Penalties-coming-for-RTHK-staff-over-June-4-stunt

[42] Rhoda Kwan, "Hong Kong's RTHK will become state media after partnership with China's CCTV, says press group chief," HKFP, August 11, 2021 https://hongkongfp.com/2021/08/11/hong-kongs-rthk-will-become-state-media-after-partnership-with-chinas-cctv-says-press-group-chief/; Reporters without Borders, "Hong Kong: RSF concerned by future "partnership" between public broadcaster RTHK and Chinese state media," August 10, 2021 https://rsf.org/en/news/hong-kong-rsf-concerned-future-partnership-between-public-broadcaster-rthk-and-chinese-state-media

[43] Jennifer Lo, "Pro-Beijing newspapers Wen Wei Po and Ta Kung Pao to merge," Nikkei Asia, February 16, 2016 https://asia.nikkei.com/Business/Pro-Beijing-newspapers-Wen-Wei-Po-and-Ta-Kung-Pao-to-merge

[44] Radio Free Asia, "China-Backed Hong Kong Paper Calls For 'Ban' on Pro-Democracy Apple Daily," April 16, 2021 https://www.rfa.org/english/news/china/hongkong-appledaily-04162021084518.html

[45] Rhoda Kwan, "Beijing-controlled paper labels Hong Kong press union an 'anti-govt political organisation'," HKFP, August 13, 2021 https://hongkongfp.com/2021/08/13/beijing-controlled-paper-labels-hong-kong-press-union-an-anti-govt-political-organisation

[46] Enoch Yiu, "Property magnate's 26-year-old daughter buys Sing Tao, sends Hong Kong paper's shares soaring by 54 per cent to five-month high," SCMP, February 2, 2021 https://www.scmp.com/business/china-business/article/3120268/shenzhen-based-kaisa-groups-kwok-hiu-ting-becomes-largest

[47] Sarah Zheng, "Hong Kong newspaper Sing Tao forced to register US arm as a foreign agent," SCMP, August 16, 2021 https://www.scmp.com/news/china/diplomacy/article/3146478/hong-kong-newspaper-sing-tao-forced-register-us-arm-foreign; Sing Tao US Registration Statement, August 23, 2021 https://efile.fara.gov/docs/6999-Exhibit-AB-20210823-1.pdf

[48] Freedom House, "China Media Bulletin 154 - May 2021"

[49] Radio Free Asia, "Publishing, Media Takeovers Part of China's Two-Pronged Grip on Hong Kong," May 10, 2021 https://www.rfa.org/english/news/china/hongkong-media-05102021083345.html

[50] Isabella Steger and Kari Soo Lindberg, "Jack Ma's SCMP Joins Hong Kong Media Groups Facing China Control," Bloomberg, March 16, 2021 https://www.bloomberg.com/news/articles/2021-03-16/jack-ma-s-scmp-joins-hong-kong-media-groups-facing-china-control

[51] Radio Free Asia, "Hong Kong's i-Cable TV Fires Dozens of Its Best Journalists ," December 1, 2020 https://www.rfa.org/english/news/china/fires-12012020093842.html

[52] John Chan, "Firings at Hong Kong TV News Network Prompt Mass Resignation," China Digital Times, December 1, 2020 https://chinadigitaltimes.net/2020/12/firings-at-hong-kong-tv-news-network-prompt-mass-resignation/

[53] Tommy Walker, "Fears About National Security Law Chill Hong Kong Media," Voice of America, August 12, 2021 https://www.voanews.com/press-freedom/fears-about-national-security-law-chill-hong-kong-media

[54] Radio Free Asia, "Hong Kong Police Charge Pro-Independence Activist Tony Chung With 'Secession'," October 29, 2020 https://www.rfa.org/english/news/china/charge-10292020092133.html

[55] Tony Cheung and Elizabeth Cheung, "Hong Kong justice secretary Teresa Cheng apologises on first day in office for controversy over 'illegal structures' in her home," SCMP, January 6, 2018 https://www.scmp.com/news/hong-kong/politics/article/2127105/hong-kong-justice-secretary-teresa-cheng-apologises-first

[56] Radio Television Hong Kong (RTHK), "Govt proposes tightening company registry searches," March 29, 2021 https://news.rthk.hk/rthk/en/component/k2/1583247-20210329.htm

[57] Selina Cheng, "Hong Kong plans to reduce transparency of electoral roll," HKFP, April 14, 2021 https://hongkongfp.com/2021/04/14/hong-kong-plans-to-reduce-transparency-of-electoral-roll/

[58] Hong Kong Journalist Association (HKJA), "2021 Annual Report: Freedom in Tatters"

[59] HKJA, "Joint-statement: Hong Kong press unions and associations sternly oppose the police's unilateral revision of its definition of media representatives under the Police General Orders," September 22, 2020 https://www.hkja.org.hk/en/statements/joint-statement-hong-kong-press-unions-and-associations-sternly-oppose-the-polices-unilateral-revision-of-its-definition-of-media-representatives-under-the-police-general-orders/

[60] Committee to Protect Journalists (CPJ), "Hong Kong denies work permit to New York Times correspondent Chris Buckley," July 15, 2020 https://cpj.org/2020/07/hong-kong-denies-work-permit-to-new-york-times-correspondent-chris-buckley/; CPJ, "Hong Kong denies work permit to editor of independent Hong Kong Free Press," August 27, 2020 https://cpj.org/2020/08/hong-kong-denies-work-permit-to-editor-of-independent-hong-kong-free-press/

[61] Michael M. Grynbaum, "New York Times Will Move Part of Hong Kong Office to Seoul," The New York Times, July 14, 2020 https://www.nytimes.com/2020/07/14/business/media/new-york-times-hong-kong.html
[62] Chris Lau, "Delayed work visas for foreign journalists in Hong Kong 'highly unusual', says press body as it warns of damage to city's reputation," SCMP, August 6, 2020 https://www.scmp.com/news/hong-kong/politics/article/3096358/delayed-work-visas-foreign-journalists-hong-kong-highly
[63] Government of the Hong Kong SAR, "Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region gazette," July 6, 2020 https://www.info.gov.hk/gia/general/202007/06/P2020070600784.htm; Patrick Frater, "National Security Law Expands Online Reach of Hong Kong Police," Variety, July 7, 2020 https://variety.com/2020/digital/asia/national-security-law-online-hong-kong-police-1234699833/
[64] "In a first under security law, Hong Kong police order telecom firms to block anti-gov't doxing website – report," HKFP, January 11, 2021 https://hongkongfp.com/2021/01/11/in-a-first-under-security-law-hong-kong-police-order-telecoms-firms-to-block-anti-govt-doxing-website/
[65] Freedom House, "China Media Bulletin 155 - June 2021"
[66] Kelvin Chan, "Hong Kong police tell foreign hosting firm to remove website," AP, June 3, 2021 https://apnews.com/article/middle-east-hong-kong-europe-police-technology-b937510d587c77249cadd5d0ff89fd7f
[67] Angeli Datt, "How Beijing Has Dismantled Freedom of Expression in Hong Kong in Just One Year," Freedom House, June 30, 2021 https://freedomhouse.org/article/how-beijing-has-dismantled-freedom-expression-hong-kong-just-one-year
[68] Su Xinqi, "A virtual Noah's Ark: Hongkongers race to archive democracy movement amid city-wide purge," Agence France Presse, August 28, 2021 https://hongkongfp.com/2021/08/28/digital-dissent-hongkongers-race-to-archive-democracy-movement/
[69] Cheng, "Security law: Stand News opinion articles axed, directors resign amid reported threats to Hong Kong digital outlets."
[70] Selina Cheng, "Hong Kong broadcaster RTHK deletes shows over a year old from internet as viewers scramble to save backups," HKFP, May 3, 2021 https://hongkongfp.com/2021/05/03/hong-kong-broadcaster-rthk-to-delete-shows-over-a-year-old-from-internet-as-viewers-scramble-to-save-backups/; Tom Grundy, "Embattled Hong Kong broadcaster RTHK deletes all Tweets, disables Twitter comments," HKFP, August 4, 2021 https://hongkongfp.com/2021/08/04/embattled-hong-kong-broadcaster-rthk-deletes-all-tweets-disables-twitter-comments/
[71] Cheng, "Hong Kong broadcaster RTHK deletes shows over a year old from internet as viewers scramble to save backups."
[72] Jack Nicas, "Apple Removes App That Helps Hong Kong Protesters Track the Police," The New York Times, October 9, 2019 https://www.nytimes.com/2019/10/09/technology/apple-hong-kong-app.html
[73] Eric Cheung, "Why Facebook is losing friends in Hong Kong," Rest of World, February 28, 2021 https://restofworld.org/2021/why-facebook-is-losing-hongkong/
[74] Hadas Gold, "Facebook, Google and Twitter won't give Hong Kong authorities user data for now," CNN, July 7, 2020 https://www.cnn.com/2020/07/06/tech/whatsapp-facebook-hong-kong/index.html; Radio Free Asia, "Facebook Turned Down Hundreds of User Data Requests From Hong Kong," June 8, 2021 https://www.rfa.org/english/news/china/hongkong-facebook-06082021103754.html
[75] "Telegram channel operator gets three-year jail sentence," The Standard, April 20, 2021 https://www.thestandard.com.hk/breaking-news/section/4/170146/Telegram-channel-operator-gets-three-year-jail-sentence
[76] Candice Chau, "Hong Kong to outlaw acts desecrating Chinese flag on the internet," HKFP, August 12, 2021 https://hongkongfp.com/2021/08/12/hong-kong-to-outlaw-acts-desecrating-chinese-flag-on-the-internet/
[77] Gao Feng, "Guangdong Dissident Poet Takes Life Amid Ongoing Police Surveillance," Radio Free Asia, July 23, 2021 https://www.rfa.org/english/news/china/suicide-07232021142253.html
[78] Joshua Wong 黃之鋒 @joshuawongcf, " 1/ Arrested on August 30, my phone was seized by #hkpolice. The phone can only be unlocked with passwords. Before court resumed yesterday, I have NEVER provided any passwords to #police, nor received any notice nor warrant for a search of my mobile device." December 19, 2019 https://twitter.com/joshuawongcf/status/1207575697633337345

[79] Lily Kuo, "Hong Kong's digital battle: tech that helped protesters now used against them," Guardian June 14, 2019 https://www.theguardian.com/world/2019/jun/14/hong-kongs-digital-battle-technology-that-helped-protesters-now-used-against-them

[80] Jon Porter, "Telegram blames China for 'powerful DDoS attack' during Hong Kong protests," The Verge, June 13, 2019 https://www.theverge.com/2019/6/13/18677282/telegram-ddos-attack-china-hong-kong-protest-pavel-durov-state-actor-sized-cyberattack; Phil Muncaster, "China's Great Cannon Fires on Hong Kong Protesters," Infosecurity Magazine, December 5, 2019 https://www.infosecurity-magazine.com/news/chinas-great-cannon-fires-on-hong/; Chris Doman, "The "Great Cannon" has been deployed again," AT&T Cybersecurity, December 4, 2019 https://cybersecurity.att.com/blogs/labs-research/the-great-cannon-has-been-deployed-again

[81] Amnesty International, "State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack," April 25, 2019 https://www.amnesty.org/en/latest/news/2019/04/state-sponsored-cyber-attack-hong-kong/; Hossein Jazi and Jerome Segura, "Chinese APT group targets India and Hong Kong using new variant of MgBot malware," Malware Bytes Lab, July 28, 2021 https://blog.malwarebytes.com/threat-analysis/2020/07/chinese-apt-group-targets-india-and-hong-kong-using-new-variant-of-mgbot-malware; Elliot Cao, Joseph C. Chen, William Gamazo Sanchez, Lilang Wu, and Ecular Xu, "Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links," Trend Micro, March 24, 2020 https://blog.trendmicro.com/trendlabs-security-intelligence/operation-poisoned-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links/; Mathieu Tartare, "Winnti Group targeting universities in Hong Kong," We Live Security, January 31, 2020 https://www.welivesecurity.com/2020/01/31/winnti-group-targeting-universities-hong-kong/; Bill Toulas, "The 'Winnti' Group of Chinese Hackers Targeted Hong Kong Universities," Tech Nadu, February 1, 2020 https://www.technadu.com/the-winnti-group-chinese-hackers-targeted-hong-kong-universities/91297/

[82] Radio Free Asia, "China's Shiny New Press Card Means Total State Control of Media: Journalists," November 11, 2020 https://www.rfa.org/english/news/china/press-11112020092314.html; Freedom House, "China Media Bulletin 151 - February 2021"

[83] China Digital Times, "Directives from the Ministry of Truth" https://chinadigitaltimes.net/china/directives-from-the-ministry-of-truth/

[84] "Hong Kong leader flags 'fake news' laws as worries over media freedom grow," Reuters, May 3, 2021 https://www.reuters.com/world/china/hong-kong-leader-flags-fake-news-laws-worries-over-media-freedom-grow-2021-05-04/

[85] Rhoda Kwan, "Hong Kong gov't and lawmakers back 'fake news' law plan; press union chief warns of new 'sword over journalists' heads'," HKFP, July 21, 2021 https://hongkongfp.com/2021/07/21/hong-kong-govt-and-lawmakers-back-fake-news-law-plan-press-union-chief-warns-of-new-sword-over-journalists-heads/

[86] The Stand News, "Digital media "852 Post" announces "closure" ; Dismissed six employees; Founder You Qingyuan: The proposed fake news law is the spark (網媒《852 郵報》宣布「暫別」 遣散六員工 創辦人游清源：擬立假新聞法是導火線)" https://www.thestandnews.com/politics/ab網媒-852郵報-宣布-暫別-遣散六員工-創辦人游清源-擬立假新聞法是導火線

[87] Office of the Privacy Commissioner for Personal Data Hong Kong, "Gazettal of Personal Data (Privacy) (Amendment) Bill 2021," July 16, 2021 https://www.pcpd.org.hk/english/whatsnew/20210714.html

[88] Chris Lau, "Hong Kong introduces new legal amendments to outlaw doxxing," SCMP, May 11, 2021 https://www.scmp.com/news/hong-kong/politics/article/3133087/hong-kong-introduces-new-legal-amendments-outlaw-doxxing; Selina Cheng, "Authorities may prosecute Hong Kong staff or ban overseas websites if they fail to remove doxxing content," HKFP, May 18, 2021 https://hongkongfp.com/2021/05/18/authorities-may-prosecute-hong-kong-staff-or-ban-overseas-websites-if-they-fail-to-remove-doxxing-content/

[89] Asia Internet Coalition, "AIC Submits Industry Letter on the Proposed Amendments to Hong Kong's Personal Data (Privacy) Ordinance to PCPD," June 25, 2021 https://aicasia.org/2021/07/05/hong-kong-aic-submits-position-paper-on-the-proposed-amendments-to-hong-kongs-personal-data-privacy-ordinance-to-pcpd/

[90] Lokman Tsui, "How tech companies should plan for Hong Kong's precarious future," Rest of World, July 28, 2021 https://restofworld.org/2021/how-tech-companies-should-plan-for-hong-kongs-precarious-future/

[91] Apple Daily, "Hong Kong national security police can seize journalistic files without court approval: prosecutors," archived at April 2, 2021 https://archive.is/sSS78

[92] Chris Lau and Cat Wang, "Hong Kong national security law: police information grab sparks fears over broad nature of powers and suspects' rights," SCMP, August 27, 2021 https://www.scmp.com/news/hong-kong/politics/article/3146542/hong-kong-national-security-law-police-information-grab
[93] "Hong Kong appoints special fraud investigator to probe defunct pro-democracy newspaper Apple Daily," AFP, July 29, 2021 https://hongkongfp.com/2021/07/29/hong-kong-appoints-special-fraud-investigator-to-probe-defunct-pro-democracy-newspaper-apple-daily/
[94] Yan Zhao and Jerome Taylor, "China's anti-sanctions law a new headache for banks in Hong Kong," AFP, August 11, 2021 https://news.yahoo.com/chinas-anti-sanctions-law-headache-031619972.html
[95] Lilian Cheng, "Hong Kong parent company of Apple Daily to cease operations on Thursday, will still try to pay staff despite authorities not releasing frozen cash," SCMP, June 30, 2021 https://www.scmp.com/news/hong-kong/politics/article/3139345/hong-kong-parent-company-apple-daily-cease-operations
[96] Selina Cheng, "Taiwan's Apple Daily scraps print edition of newspaper after 18 years," HKFP, May 14, 2021 https://hongkongfp.com/2021/05/14/taiwans-apple-daily-scraps-print-edition-of-newspaper-after-18-years/

OPENING STATEMENT OF SAMUEL CHU, FOUNDER AND FORMER MANAGING DIRECTOR, HONG KONG DEMOCRACY COUNCIL

VICE CHAIRMAN CLEVELAND: Thank you, so much, Ms. Datt, a powerful statement. Mr. Chu?

MR. CHU: Thank you Co Chairs and Commissioners for hosting this hearing and for the opportunity to speak and testify to you today, and to my fellow panelists, who I think both bring incredible expertise and experience to the subject. I want to focus my remarks on the swift and complete closing of Hong Kong civil society space in the past year, what crackdowns might be forthcoming, and what the U.S. can do and should do in response.

For 30 years, Hong Kong Alliance, the group that behind the annual June 4th Vigil in Victoria Park. It was a vigil that was attended by thousands. And for 30 years, it was the only such public event on Chinese soil. That was until last year, when the Hong Kong government banned the gathering citing COVID 19 concerns. And it did so again this year. Early morning, yesterday in Hong Kong, four of the steering committee members of the Hong Kong Alliance were arrested at their homes after the group have refused to hand over the membership and financial records during a National Security Police investigation. We might never witness another June 4th vigil in Hong Kong again. In 2019, many of us were captivated by millions of Hong Kongers who marched people peacefully week after week. The vigils and the tactics spilled over across the regions and inspired other anti-authoritarian and pro-democracy protests movements in the world. We might never witness another peaceful protest march in Hong Kong again. And this might be the most observable sign of the demise of Hong Kong civil society, is the complete and abrupt end of all peaceful public protests. Under COVID pandemic measures and using a seldomly used colonial era Public Order Ordinance, Hong Kong authorities have effectively banned all public gatherings, marches, rallies, vigils, and criminalized the freedom of assembly. And this is especially significant for Hong Kongers because in a city without a democratic representative government, mass protest has been the most effective, visible, consistent, civil society tactic over time.

Today, all protests and public expression of events are deemed as "unauthorized assembly". The charge of unauthorized assembly is based on a Public Order Ordinance and punishable for up to five years in prisons. And this has been used to imprison young activists like Joshua Wong, Agnes Chow, and Ivan Lam, Jimmy Lai, owner and publisher of the opposition paper Apple Daily, top labor leader Lee Cheuk-yan, and dozens of former lawmakers all for participating, organizing, or inciting an unauthorized assembly. Former lawmakers and barristers, Margaret Ng and Martin Lee received suspended sentence, which de facto serves as house arrest and gag orders, prohibiting them from participating in civil society, or speaking to media, or international groups.

In all, over 10,000 people have been arrested in protest related charges since 2019. And then, last month, the Civil Human Rights Front, the broad-based organization behind all the largest protests in the city since 2002 announced it would disband after the government threatened to investigate the group under National Security Law. But CHRF was only one example of the systemic dismantling of civil society institutions in Hong Kong this year. Because the National Security Law, the NSL, has proven to be the perfect weapon against the

civil society. As Michael, as Professor Davis mentioned, the NSL punishes four different types of activity: succession, subversion, terrorism, and collusion with "foreign forces." And all of them carrying a maximum sentence of life in prisons.

Though vaguely defined, they have become catch all offenses to detain activists and to dismantle civil society groups. Freedom of expressions or speech has now been criminalized as seditious. International engagement, including with the U.N., or U.S. Congress, or overseas diaspora groups, is cast as colluding with foreign forces. Fundraising by or donating to pro-democracy organizations could be investigated. Organizational accounts and assets could be frozen and seized without due process. These arrests have fundamentally altered the environment for civil society groups to operate. They have stoked fears for persecution. And as a result, groups that have chosen to "voluntarily" disband, including professional organizations like the Union for New Civil Servants, Frontline Doctors Union, the Progressive Lawyers Group.

Last week, the Hong Kong Pastors Network, a group of Christian clergy who has organized numerous prayer vigils in support of the protests, even announced it too has ceased operation and disbanded. And over just three weeks in August, the Hong Kong Professional Teachers' Union, the largest teachers' union representing the 95,000 teachers in the city; the 612 Humanitarian Fund, which has distributed over 243 million Hong Kong dollars to protesters facing prosecutions and financial hardship; and the Civil Human Rights Front, organizers of the annual July 1 rally since 2002. All announced they would voluntarily disband. And they've all encountered a similar pattern of threats and attacks. They were called a malignant tumor, the teachers' unions in the pro-Beijing newspapers. They face arbitrary investigations as the civil rights human rights front were told by police after 19 years of receiving permission to march, they now we're breaking the law for not having registered with the police themselves.

Using COVID measures, Beijing and Hong Kong authorities have all intended purposes, close the space for civil society. Hong Kongers now live in a self-described white terror. Last November, police launched a tip line for residents to report suspected national security violations. It registered 100,000 reports in the first six months. In June, police arrested a 37-year-old man on suspicion of sedition after an anonymous tip reported that the sticker he put on his apartment door might have violated national security. By turning neighbors, coworkers, and even family into informants, the government is not only sniffing out all the collective public actions, but the everyday activities of individuals. And it doesn't end at the border. The NSL details how foreign nationals committing acts outside of Hong Kong and China are still criminally liable.

This claim of extraterritorial jurisdiction led to the arrest warrant that was issued against me and five others, making me the first U.S. citizen last year to be targeted. The threat to civil society groups extends overseas as illustrated by the recent sanctions, the use of the new anti-sanction laws by the Ministry of Foreign Affairs against the organization I founded. I will leave you to read the recommendations around what will happen and what will continue to happen. But I do want to end on a personal note.

As I mentioned, the Alliance were, had their leaders arrested just recently. I was there when the Alliance was formed in 1989 during a march of the first million Hong Kongers on May 21st. My father served with those steering committee members for 30 plus years. It was through the Alliance that my Dad helped launch a smuggling operation that saved 400 dissidents from

Tiananmen Square back in '89. Fearing retribution, my father sent me to the U.S. to study and live here. But I returned to Hong Kong over the years to June 4th vigils in Victoria Park.

In 2014, my father, and Benny Tai, and Chan Kin Man started Occupy Central, the civil disobedience campaign that led to the Umbrella Movement. They were later arrested, tried convicted, and sentenced to jail. And after the trial, I came back to the U.S. and started Hong Kong Democracy Council where I served as Managing Director until recently. And then became, one, a fugitive and a sanctioned organization in just two short years. For me, and for so many Hong Kongers, civil society is personal and generational. It is actually how we mark the passage of time and history as Hong Kongers.

Chow Han- tung, who's the Vice Chair, the only one who was left, until yesterday, free on bail was asked earlier this summer about being attacked for saying, ending one party rule as a slogan for the Hong Kong Alliance and as part of its core mission. And if they would consider abandoning that slogan and that mission to appease the authorities, Chow in response stated defiantly and simply, if we change that we are not us anymore. We haven't given up and we ask that you and the world not give up on us. Thank you.

PREPARED STATEMENT OF SAMUEL CHU, FOUNDER AND FORMER MANAGING DIRECTOR, HONG KONG DEMOCRACY COUNCIL

September 8, 2021
Samuel M. Chu
Founder/Former Managing Director, HKDC

Testimony before the U.S.-China Economic and Security Review Commission
"U.S.-China Relations in 2021: Emerging Risks"
Panel I: Beijing's Assertion of "Comprehensive Jurisdiction" over Hong Kong

Thank you, co-chairs, and commissioners for the opportunity to testify today.

I want to focus my remarks on the swift and complete closing of Hong Kong's civil society space in the past year, what further crackdowns could be forthcoming, and what the US can do in response.

Let me preface that what is happening in Hong Kong is not isolated; it mirrors an alarming, decade-long global trend. Closing space for civil society takes various forms: incarceration, regulations, restrictions on funding, limits to freedom of speech, digital and physical harassment, and even murder. It is unfolding in every part of the world.

The International Center for Not-for-Profit Law reported that since 2013, 103 countries had proposed more than 340 legislative initiatives that impact civil society. Of those, 244 were restrictive (72%).

For example, on August 20, 2021, Ugandan authorities announced without warning that they had halted the operations of 54 civil society and human rights groups.

Currently, the Russian Ministry of Justice lists 43 media outlets, journalists, and 76 civil society groups as "foreign agents." An additional 46 groups have been labeled "undesirable organizations."

Between February and May 2021, senior Salvadorian government officials perpetrated more than 370 digital attacks on social networks against human rights defenders. Bertha Deleón, a women's rights lawyer, has faced a mass intimation and stigmatization campaign as well as criminal prosecution, leading her to request precautionary measures and protection from the Inter-American Commission on Human Rights (IACHR).

In the Philippines, human rights defenders and indigenous activists face threats daily as they attempt to defend their land peacefully. In the first six months of 2021, 15 human rights defenders have been murdered.

There are, however, characteristics of the crackdown on civil society specific to Hong Kong and its unique history and status as a Special Administrative Region (SAR) of the People's Republic of China (PRC).

Perhaps the most observable sign of the demise of Hong Kong's civil society is the complete and abrupt end to all peaceful public protests.

The world has been mesmerized by the images of up to 2 million Hong Kongers peacefully marching week after week in 2019. The visuals and tactics from the streets of Hong Kong spilled across the region and inspired other anti-authoritarian, pro-democracy protest movements in Thailand, Burma, and, most recently in Afghanistan.

For more than 30 years, Hong Kongers held the annual vigil commemorating the June 4 Tiananmen massacre, the only one on Chinese soil. This year, authorities banned the annual Tiananmen massacre vigil for a second straight year, citing coronavirus social distancing restrictions.

We might never witness any of them again.

Hong Kong authorities, aided by the COVID pandemic and zealous use of colonial-era Public Order Ordinance (POO), have effectively banned all public protests, rallies, vigils and criminalized the freedom of assembly.

The protest ban is especially significant for Hong Kongers because consistently, over time, mass, peaceful protests have been the most visible, effective, consistent civil society tactics in a city without a representative government.

However, since January 2020, the government has put a blanketed end to public protest by declaring them "unauthorized assembly."

The charge of "unauthorized assembly," punishable by up to five years in prison, is based on the Public Order Ordinance (POO). It requires organizers of demonstrations of more than 30 people to notify police seven days in advance. It also requires organizers to get a letter or "notice of no objection" from the police.

No "notice of no objection" has been granted to protest groups in the city since January of 2020. At the same time, POO has been used aggressively to target prominent and leading civil society actors.

On December 2, 2020, leading activist Joshua Wong was sentenced to 13.5 months for organizing and inciting a June 2019 "unauthorized assembly." Fellow activists Agnes Chow and Ivan Lam were also sentenced to 10 and 7 months for "incitement," based on evidence that they shouted slogans using a loudspeaker at the same protest. In May 2021, Wong, already in jail, was sentenced to an additional ten months for attending the annual June 4 vigil in 2020.

In April 2021, ten prominent pro-democracy figures were sentenced to between 8 and 18 months for participating in two "unauthorized assemblies" in August 2019. The group included Jimmy Lai, the owner, and publisher of the opposition newspaper Apple Daily, top labor leader Lee Cheuk-yan and three other former opposition lawmakers.

The court also handed down suspended sentences to former lawmakers and barristers Margaret Ng, Albert Ho, and Martin Lee - the "founding father" of the pro-democracy movement and the founding chair of Hong Kong's Democratic Party.

The suspended sentences have served as a de facto "political house arrest" and gag order – prohibiting their participation and involvement in any protest or civil society activities and contacts with international media and entities during their jail terms.

On May 28, 2021, Jimmy Lai, Lee Cheuk-yan, and Leung Kwok-hung were all given new sentences between 14 and 18 months for organizing another "unauthorized assembly" on October 1, 2020. Figo Chan, the convener of the Civil Human Rights Front (CHRF), the group behind many of the largest protests since 2002, was sentenced to 18 months.

In all, over 10,000 have been arrested for protest-related charges and 2,600 prosecuted since the start of the anti-extradition protest in 2019.

The final nail in the coffin came last month, when the Civil Human Rights Front (CHRF), the broad-based organization that once boasted more than 60 civil society groups as members and the organizer behind all the largest peaceful public protests in the city since 2002 - announced it would disband under threats of investigation and prosecution by the government.

The dissolution of CHRF is only one example of a broader, systemic dismantling of core and foundational civil society organizations.

The National Security Law has proven to be the perfect weapon against Hong Kong's civil society - forcing the self-censoring and disbanding of groups new and old. But, most importantly, the threat of NSL violations has dismantled the foundation of Hong

Kong's civil society by eliminating some of the oldest, most prominent, and most influential civil and mediating institutions in Hong Kong's history.

NSL punishes four types of activities: secession (Articles 20-21), subversion (Articles. 22-23), terrorism (Articles 24-28), and collusion with "foreign forces" (Articles 29-30), all carrying a maximum sentence of life in prison.

But in the hands of the national security forces, they have become vaguely defined, catch-all offenses to prosecute individual activists and civil society leaders while also forcing groups to self-censor and disband.

The authorities have done this by criminalizing freedom of expression as "sedition," cast legitimate international engagement, including to the United Nations or diaspora Hong Kong groups, as "collusion with foreign forces."

Fundraising by and donating to pro-democracy organizations or protest-related campaigns could be investigated as an NSL crime, leading to account and asset freeze and seizures.

The NSL established new PRC national security offices in Hong Kong while also giving Hong Kong police sweeping, unchecked powers, including warrantless searches, covert surveillance, and seize travel documents and deny bail of those suspected of possible future acts against national security.

In total, at least 154 individuals have been arrested under the NSL - a majority of those arrested languish behind bars without bail.

These arrests have fundamentally altered the civil society space and stoke fears for future prosecution among civil society groups and actors. As a result, many civil society groups have chosen to disband voluntarily:

January 16: **The Union for New Civil Servants** disbanded after officials threatened to dismiss workers refusing to pledge fealty to the Chinese Communist Party and "protect national security."

June 2: **The Good Neighbor North District Church**, which has aided protestors, disbanded after the police froze its bank account on suspicion of money laundering

June 28 and 30: Two major medical professional groups **Frontline Doctors Union** and **Médecins Inspirés**, both active and vocal against the government responses to the protest and COVID, announced they would disband

July 6: The **Progressive Lawyers Group (PLG)**, founded in 2015, disbanded

August 10: The **Hong Kong Professional Teachers' Union (HKPTU)**, Hong Kong's largest teachers' union representing 95,000 members and 90% of the teachers in the city, announced they would dissolve after 47 years of operations

August: **612 Humanitarian Relief Fund** announced it would cease operation by October 31. It has distributed more than HK$243 million (US$31.2 million) to protesters facing prosecution or financial hardship because of the protest movement since 2019

August 13: **Civil Human Rights Front (CHRF)**, organizer of some of the largest protests, announced they would disband

August: **Hong Kong Alliance in Support of Patriotic Democratic Movements of China**, the group behind the annual June 4 vigil since 1989, announced it would dissolve. Despite that, last week, the police's national security unit accused the Alliance of being "an agent of foreign forces" and demanded information about its membership, finances, and activities.

September 3: **Hong Kong Pastors Network**, a group of Christian clergy, who organized numerous prayer vigils in support of the protest movement, announced it has ceased operations and disbanded.

Many of the disbanded groups encountered a similar pattern of threats, attacks, and government investigation.

Pro-Beijing media, sometimes Hong Kong government officials, would publicly criticize and suggest that a group's activities might have run afoul of the NSL. The Professional Teachers' Union (PTU) was described by CCP mouthpieces the *People's Daily* and Xinhua as **"a malignant tumor."** Hours later, the government cut ties with the union, announcing that officials would no longer consult and cooperate with them on matters of mutual concern. Days later, PTU announced it would dissolve.

Groups also faced arbitrary and irregular government investigations. Though Civil Human Rights Front (CHRF) had organized marches with police permission for 19 years, Hong Kong Police Commissioner Raymond Siu suggested in an interview with pro-Beijing newspapers that **CHRF broke local laws by not registering as a company with the Companies Registry and as a legal society with the police force.**

This week, police obtained court orders under NSL to require the 612 Humanitarian Relief Fund to disclose its source of donations, donor information, and the purpose of donations. The fund has distributed more than HK$243 million (US$31.2 million) to protesters facing prosecution or financial hardship because of the protest movement since 2019

But by far, the largest group of NSL arrests and prosecution came against those who organized and took part in the June 2020 Legislative Council (LegCo) primaries. **The primaries were conceived and implemented as a civil society-led process to build engagement and leverage in a decisively undemocratic general election process.**

Furthermore, those arrested were not merely traditional politicians - they are leaders and organizers from labor, journalists, LGBT, ethnic minorities, women's rights, sending a chill across the full spectrum of civil society groups.

I was also asked by the Commission to briefly address **the impact of NSL and its complete capture of the education system in Hong Kong.**

Since 2019, authorities have begun **deregistering teachers** for introducing protest or pro-democracy-related themes or materials in the classroom. Others were targeted for their protest participation or political views shared online outside classrooms and schools. 269 complaints accusing teachers of misconduct have been filed from June 2019 to December 2020, and 154 have been disciplined - many of them based on anonymous complaints.

Earlier this year, the government announced the **imposition of national security education** as part of the "necessary measures to strengthen public communication, guidance, supervision, and regulation over matters concerning national security, including those relating to schools, universities, social organizations, the media, and the internet."

Students as young as 6 years old will learn how to sing and respect China’s national anthem and be taught what constitutes offenses such as “sedition” or “collusion” and their associated and appropriate penalties.

The Education Bureau has issued a new curriculum designed to instill "affection for the Chinese people"; geography lessons must affirm China's claim over disputed areas of the South China Sea. Bringing a copy of the newspaper Apple Daily to the classroom or teaching a class about the 1989 Tiananmen protest could mean a lifetime ban from teaching.

The total capture of the education does not confine to the classrooms and official curriculum.

Five members of the General Union of Hong Kong Speech Therapists were arrested in late July. They were subsequently remanded in custody after being charged with "sedition" over a series of children's books about sheep defending their village from invading wolves. The government accused them of "inciting" hatred against the government.

And as noted, HKPTU, the single largest trade union in Hong Kong with 95,000 members (90% of the city's teachers), was forced to dissolve, citing enormous political pressure.

Using COVID health measures and Public Order Ordinance to outlaw public protests and wielding the threat of NSL prosecutions to uproot and bulldozed foundational civil society groups, the space for civil society in Hong Kong has, for all intent and purposes, been closed.

Hong Kongers now live in a self-described "white terror," extending far beyond the traditional civil society spaces.

Two other features illustrate how far-reaching and total the closure of civil society space in Hong Kong has been.

On November 5, 2020, police launched a "tip line" for residents to report suspected NSL violations. The phone line registered more than 100,000 messages in the first six months. In June, police arrested a 37-year-old man on suspicion of "sedition" after receiving anonymous tips that stickers he placed on the gate to his apartment potentially violated the NSL. **By turning neighbors, coworkers, and even family members into monitors and informants, the authorities are snuffing out not only collective, public actions but also controlling individual and everyday activities of individuals.**

Lastly, the closure and crackdown do not end at the borders. The NSL (Article 38) details how foreign nationals committing acts outside Hong Kong and China are criminally liable under the law. Such foreigners could be arrested upon arrival in Hong Kong. This claim of **extraterritorial jurisdiction** was the basis of the arrest warrants issued against me, a US citizen, last July. The **harassment and threats to civil society groups and individuals extend overseas,** as illustrated by the recent sanction by the PRC Ministry of Foreign Affairs against the US organization I founded supporting the movement.

What changes are forthcoming?

Pro-democracy and civil society leaders will continue to be prosecuted and detained.

The attacks on civil society groups will also continue. Last month, Chief Executive Carrie Lam warned the Law Society of Hong Kong days ahead of its leadership election that if the group's "professional role is overridden by politics, the government will consider severing its relationship with it."

Beijing will "astroturf" a state-sponsored "grassroots" sector. As part of Beijing-imposed election process, hundreds of new groups, with names like “Modern Mammy Group” or “Sea Bear Swimming Club”, and the “Sea Bear Squash Club” registered at the same address will now be allowed to help select the new chief executive.

It will take a concerted effort to preserve and restore Hong Kong's civil society - and the US can and must play a leading role.

The US must raise the profile of the role of civil society and the closing space issue by continuing to monitor restrictions, increase Consulate involvement, and highlight the issue at high-profile events such as the upcoming White House Summit for Democracy in December.

Respond to any civil society crackdown and attacks with targeted sanctions and public condemnation.

Reconstitute the interagency working group on civil society and roles such as the State Department's Senior Advisor for Civil Society and Emerging Democracies to coordinate programs and policies impacting civil societies globally.

Continue to provide **emergency financial support in response to threats** against civil society activists via programs like Lifeline Embattled CSO Assistance Fund. Extend those support to activists overseas.

Require reporting and briefing on whether the Chinese government and affiliated entities have engaged in **intimidation or harassment of any groups and individuals** in the US.

Fund civil society abroad. Congress recently included a $10 million appropriation request to strengthen the pro-democracy movement in Hong Kong. The US must adapt more sensitive and flexible funding methods consider investing in diaspora groups.

Welcome civil society leaders fleeing Hong Kong through temporary and permanent status, visa, refugee, asylum, and humanitarian support.

Expand **peer-to-peer exchanges** between the US and Hong Kong.

The rapid and complete closing space for civil society is not abstract or merely academic.

I marched in the first million Hong Kongers' protest supporting Tiananmen students on May 21, 1989. During that march, the Hong Kong Alliance was formed. My father, the Rev. Chu Yiu Ming, served on its standing committee from that day until last year. He did so alongside Szeto Wah, the founding chair of both the Alliance and the Teachers' Union until his passing in 2011.

Through the Alliance, my father helped launch "Operational Yellowbird" - the smuggling operation that rescued 400 activists who escaped the Tiananmen massacre. Fearing retribution, my father sent me to study and live in the US. But I returned to Hong Kong over the years to light candles at the June 4 vigils at Victoria Park organized by the Alliance.

In 2014, I joined my father at Occupy Central, the civil disobedience campaign he co-founded with Benny Tai and Kin Man Chan that grew into the Umbrella Movement. They were later arrested, tried, convicted, and sentenced to jail.

After their trial in 2019, I returned to DC and launched the Hong Kong Democracy Council, where I served as managing director until recently. Our organizing and advocacy made us one of the most frequent targets of CCP's rage and retaliation.

For me - and so many Hong Kongers - Hong Kong's civil society is personal and generational. It is how we mark the passage of time and history as Hong Kongers.

We must preserve the memories, artifacts, and talents in this critical moment.

Chow Hang-tung, a barrister and vice-chair of the Alliance, is one of the few leaders still free on bail while awaiting trial. Two weeks ago, the government launched an investigation into the Alliance, accusing its leaders of being "foreign agents" and demanding information on membership and finances.

Pro-Beijing mouthpieces have attacked one of the group's slogans and core mission - "ending one-party rule" - as being seditious and subversive. When asked if the group would ever consider abandoning the slogan and goal to appease the authorities, Chow stated defiantly and simply that:

"If we change that, we are not us anymore."

We have not given up, and we ask that the world not give up on us.

OPENING STATEMENT OF MAUREEN THORSON, PARTNER, WILEY LAW

VICE CHAIRMAN CLEVELAND: You leave me speechless, Mr. Chu. So I'm going to turn to Ms. Thorson. But thank you for your statement. Ms. Thorson?

MS. THORSON: Good morning, thank you. My thanks to the Commission for inviting me to speak today regarding the effects of China's assertion of dominance over Hong Kong on the United States import trade. My testimony focuses on the potential for Hong Kong to be used as a transshipment hub for Chinese origin goods in a bid to avoid U.S. import duties. I'll start with a brief overview of the United States current trade relationship with both Hong Kong and China as concerns import matters.

For many years after the 1997 handoff of Hong Kong to China, the United States treated Hong Kong as an entirely separate customs territory. This meant that importers bringing goods produced in Hong Kong to the United States declared and marked the goods as having Hong Kong origin rather than Chinese origin. Any duties owed on the goods were also collected with the understanding that the goods were not Chinese. In 2020, the United States ceased allowing imported goods produced in Hong Kong to be marked as goods of Hong Kong, rather than goods of China. However, the United States has continued not to treat goods produced in Hong Kong as Chinese for duty collection purposes. In other words, duties owed on Chinese origin goods are not levied on goods produced in Hong Kong.

In July of 2018, the United States began imposing additional import duties on Chinese origin products pursuant to Section 301 of the Trade Act of 1974. The duties have been imposed on four successive tranches of products each identified by their classification under the Harmonized Tariff Schedule of the United States. Collectively, the duties which range from 7.5 to 25 percent, affect goods accounted for hundreds of billions of dollars in annual import trade with China. As the Commission knows, China has thought to increase its control over Hong Kong in recent years. Given this trend, as well as the substantial U.S. import duties attaching to Chinese goods, there has been concern that Chinese companies would seek to use Hong Kong to avoid duty liability.

One of the primary concerns has been with the potential for the transshipment of Chinese products through Hong Kong. In a transshipment scheme, goods of one country are sent to another where they are repackaged and relabeled to falsely reflect the origin in the new country prior to further shipment to a final import destination. To assess whether Hong Kong is being used as a transshipment hub, I reviewed trends and U.S. imports of goods from Hong Kong both before and after the imposition of Section 301 duties on Chinese goods. In 2017, they are immediately preceding the first 301 duties. U.S. imports from Hong Kong totaled $6.8 billion, which fell to $6.1 billion in 2018, and fell further to $4.6 billion in 2019. Airport volumes then spiked in 2020 to $7.9 billion. However, the spike is attributable to a massive upswing in imports of gold in April and May. Notably, U.S. imports of gold from all countries sources increased dramatically in the spring of 2020, as the economic uncertainty caused by the coronavirus pandemic shook global financial markets. After this spike, U.S. imports from Hong Kong fell back. On an annualized basis, imports from Hong Kong are projected to reach only $3.6 billion this year, their lowest level since 2009, in the middle of the global recession.

To the extent that Chinese companies chose to use Hong Kong as a transshipment hub for evading Section 301 duties and other U.S. duties specific to Chinese products, one would expect increased exports from Hong Kong coinciding with the imposition of these duties. The recent import data does not reflect such an increase. However, Hong Kong was a known transshipment

hub in the past, particularly for textile products. And transshipment of Chinese origin goods to avoid Section 301 duties, as well as anti-dumping, and countervailing duties is a significant problem with respect to imports from countries such as Vietnam, Thailand and Malaysia.

In my written testimony, I review recent import trends from these countries and briefly explain why they are indicative of significant transshipment of Chinese goods. To combat existing transshipment and forestall future evasion scams, the United States should consider taking several actions.

First, the United States should provide increased funding to U.S. Customs specifically aimed at investigating and addressing transshipments. While Customs already has the authority to investigate and penalize transshipment schemes, the problem is large enough to merit increased funding specific to transshipment.

Second, the United States should consider expanding customs authority under the Enforce and Protect Act to include evasion of Section 301 and other similar duties, such as those imposed under Section 232 of the Trade Expansion Act of 1962.

While Customs have general authority to investigate and penalize import related fraud under 19 USC 1592, the separate Enforce and Protect Act provides a special mechanism for combating the evasion of antidumping and countervailing duties. Using this mechanism, the Agency has been able to quickly shut down duty evasion schemes. The mechanism also provides enhanced public visibility into the identity of bad actors complicating their ability to simply adjust their schemes and continue with them. Notably, many of the more than 130 investigations that Customs has conducted so far under the Enforce and Protect Act have involved transshipment schemes.

Finally, the United States should consider amending 19 USC 1592(a). This statute requires Customs to publish at least twice a year, the identities of persons who have been penalized for transshipment of textile products. This requirement could be applied more broadly to the transshipment of any type of product, providing importers with visibility into foreign companies engaged in fraudulent transshipment schemes.

To conclude, while Hong Kong does not yet appear to be a major hub for transshipment of Chinese origin goods, the transshipment of Chinese products to avoid lawful import duties is a serious problem. Luckily, there are concrete steps that the United States can take to cut down on such transshipment. I'm happy to answer any questions that the Commission may have. Thank you.

PREPARED STATEMENT OF MAUREEN THORSON, PARTNER, WILEY LAW

wiley

Testimony before the U.S.-China Economic and Security Review Commission, U.S.-China Relations in 2021: Emerging Risks

U.S. Trade with Hong Kong and the Potential for Duty Evasion, September 8, 2021

Maureen Thorson, Partner, Wiley Rein LLP[1]

I. Introduction

This testimony focuses on the how the United States' import trade with Hong Kong has shifted in recent years, and the extent to which recent trade flows suggest evasion of U.S. import duties, particularly duties applicable to Chinese-origin merchandise under Section 301 of the Trade Act of 1974.

I begin with a background discussion of recent developments in the United States' treatment of imports from Hong Kong, including the suspension of certain special treatment accorded to Hong Kong under the United States-Hong Kong Policy Act of 1992. I also discuss the imposition of Section 301 duties on goods of China, and how this has incentivized Chinese producers and exporters, and unscrupulous U.S. importers, to engage in duty evasion schemes.

Next, I review historical and recent trends in imports into the United States from Hong Kong, focusing on how trade flows from Hong Kong have shifted since Section 301 duties were first imposed on Chinese-origin goods. I discuss the extent to which these data suggest that goods of Chinese origin are being transshipped through Hong Kong and other Southeast Asian countries, in a bid to conceal their origin and avoid lawful U.S. import duties. While these data do not suggest – yet – that Hong Kong is a major transshipment hub, the territory has been used as a transshipment hub in the past, particularly with respect to textiles. Further, transshipment writ large is a substantial problem, with Chinese companies going to great lengths to conceal the origin of their goods by transshipping them through countries like Vietnam.

To combat existing and future transshipment, the United States should consider at least three strategies. These include (1) increased funding for transshipment-focused targeting and enforcement; (2) expanding the reach of the Enforce and Protect Act (EAPA) to cover action to evade Section 301 duties; and (3) implementing new legislation similar to the existing 19 U.S.C. § 1592a,to "name-and-shame" transshippers and raise awareness in the trade community as to the companies engaging in the practice.

[1] This testimony reflects the personal views of the author and not necessarily the views of her firm or the firm's clients.

II. Recent Developments in the United States' Trade and Tariff Treatment of Hong Kong

In 1992, five years in advance of the return of Hong Kong to Chinese sovereignty, Congress enacted the United States-Hong Kong Policy Act.[2] The Act reflected Congress's position that the United States should continue to "respect Hong Kong's status a separate customs territory" and a signatory in its own right to the General Agreement on Tariffs on Trade, which forms the backbone of the World Trade Organization agreements.[3] However, the Act also provided the President of the United States with authority to declare, at any time on or after July 1, 1997, that Hong Kong was no longer sufficiently autonomous to justify special treatment under a particular U.S. law, and to suspend such treatment.[4] In 2019, the Act was amended to require the Secretary of State to report annually to Congress regarding Hong Kong's autonomy and status.[5]

On May 28, 2020, then-Secretary of State Mike Pompeo released the annual Hong Kong Policy Act Report for 2020.[6] In that report, the Secretary stated that he could "no longer certify that Hong Kong continues to warrant" treatment different from China under U.S. law.[7] Secretary Pompeo pointed specifically to the erosion of political liberties in the territory, as well the Chinese government's May 22, 2020 announcement that it would soon impose new national security legislation on Hong Kong.[8] On the same day that Secretary Pompeo issued his report, China's National People's Congress approved the enactment of this national security legislation.[9]

On July 16, 2020, then-President Trump issued Executive Order 13936, titled "The President's Executive Order on Hong Kong Normalization."[10] In that order, the President declared that Hong Kong was no longer sufficiently autonomous to warrant treatment distinct from that of China for certain purposes.[11] He stated that the United States' policy, going forward, "shall be to suspend or eliminate differential and preferential treatment for Hong Kong to the extent permitted by law."[12] In the Executive Order, the

---

2 United States-Hong Kong Policy Act, Public Law 102-383 (Oct 5, 1992), 106 Stat. 1448.
3 *Id.* at Section 102.
4 *Id.* at Section 202.
5 Hong Kong Human Rights and Democracy Act of 2019, Public Law 116-76 (Nov. 27, 2019).
6 U.S. Department of State, *2020 Hong Kong Policy Act Report* (May 28, 2020), *available at* https://www.state.gov/2020-hong-kong-policy-act-report/.
7 *Id.*
8 *Id.*
9 Congressional Research Service, *Revoking Hong Kong's Preferential Trade Status: Legal Framework and Implications* (Apr. 2, 2021) at 1, *available a*t https://fas.org/sgp/crs/row/LSB10488.pdf.
10 *The President's Executive Order on Hong Kong Normalization*, E.O. 13936, 85 Fed. Reg. 43,413 (July 14, 2020) ("Executive Order 13936").
11 *Id.* at 43,413.
12 *Id.* at 43,414.

President specifically suspended special treatment for Hong Kong under 19 U.S.C. § 1304,[13] a statute that requires goods imported into the United States to be marked with their country of origin.[14] However, the Executive Order did not require Hong Kong to be treated equivalently with China for purposes of special import duties, such as the duties imposed on Chinese-origin products under Section 301 of the Trade Act of 1974.[15]

U.S. Customs and Border Protection ("CBP") subsequently issued Cargo Systems Message 43633414 on August 11, 2020.[16] The agency stated that it would provide importers with a transition period lasting until September 25, 2020 in which to adjust the marking of goods produced in Hong Kong to reflect China as the country of origin.[17] CBP's message did not indicate that products of Hong Kong would be treated as Chinese for purposes of Section 301 duties.[18] CBP later posted guidance to its website confirming that Section 301 duties were not applicable to goods produced in Hong Kong.[19]

Hong Kong subsequently filed a complaint against the new marking requirements with the World Trade Organization.[20]

III. The Imposition of Section 301 Duties on Chinese-Origin Goods

On August 24, 2017, at the request of the President, the Office of the U.S. Trade Representative ("USTR") initiated an investigation under Section 301 of the Trade Act of 1974 into the Government of China's acts, policies, and practices related to technology transfer, intellectual property, and innovation.[21] Consistently with Section 301, the investigation sought to determine whether the investigated practices were unreasonable or discriminatory, such that they burdened or restricted U.S. commerce.[22] After

---

13 *Id.*

14 19 U.S.C. § 1304.

15 *See* Executive Order 13936.

16 CSMS # 43633412 – GUIDANCE: New Marking Rules for Goods Made in Hong Kong – Executive Order 13936 (August 11, 2020), *available at* https://content.govdelivery.com/accounts/USDHSCBP/bulletins/299cb04.

17 *Id.*

18 *Id.*

19 U.S. Customs & Border Protection, "Section 301 Trade Remedies Frequently Asked Questions," *available at* https://www.cbp.gov/trade/programs-administration/entry-summary/section-301-trade-remedies/faqs.

20 *See, e.g.*, WTO *Dispute Settlement Proceeding Regarding United States – Origin Marking Requirement (Hong Kong, China)*, 86 Fed. Reg. 13,960 (USTR Mar. 11, 2021). Hong Kong alleges that the marking requirement violates various articles of the General Agreement on Tariffs and Trade, the Agreement on Rules of Origin, and the Agreement on Technical Barriers to Trade. The WTO's Dispute Settlement Body established a panel to consider the complaint on April 30, 3021.

21 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (82 Fed. Reg. 40,213 (USTR Aug. 24, 2017)) (initiation of Section 301 investigation).

22 *Id.*

collecting written comments and holding a hearing, USTR issued a report on March 22, 2018, in which it found a variety of Chinese policies and practices to be unfair and burdensome.[23] On April 6, 2018, USTR published a notice of its determination in the *Federal Register*, and indicated that it proposed to take action by imposing additional duties on a range of Chinese goods.[24]

Ultimately, duties were applied in four stages. For each stage, duties were applied to specific goods based on tariff line – that is, the eight-digit classification of specific goods under the Harmonized Tariff Schedule of the United States ("HTSUS").[25] The first stage, often termed "Tranche 1," covered tariff lines accounting for approximately $34 billion in yearly imports from China.[26] Duties became effective at a rate of 25% as to Tranche 1's tariff lines on July 6, 2018.[27] The tariff lines covered by Tranche 1 were primarily located in Chapters 84 and 85 of the United States' tariff schedule, covering machinery and electronics.[28] The "Tranche 2" duties, covering additional tariff lines accounting for approximately $16 billion in yearly imports of Chinese goods, went into effect at a duty rate of 25% on August 23, 2018.[29] This tranche included tariff lines associated with additional machinery, plastics, certain vehicles, and optical and measuring devices.[30] The "Tranche 3" duties, covering additional tariff lines accounting for approximately $200 billion in annual imports, went into effect on September 24, 2018, at a duty rate of 10%.[31] This tranche covered a broad range of goods including foods, chemicals, wood products, leather, certain textiles, metals and metal products, but did not cover apparel or footwear.[32] Duties were raised on goods subject to this tranche effective May 10, 2019, with a short grace period for goods that had already been exported from China by May 10.[33] The fourth tranche of duties covered a similarly broad range of goods,

---

23 Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* Under Section 301 of the Trade Act of 1974 (Mar. 22, 2018), *available at* https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.

24 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 14,906 (USTR Apr. 6, 2018) (notice of determination and request for public comment concerning proposed determination of action pursuant to Section 301).

25 *See, e.g., China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 28,710 (USTR June 20, 2018) (notice of action and request for public comment concerning proposed determination of action pursuant to Section 301).

26 *Id.*

27 *Id.*

28 *Id.*

29 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 40,823 (USTR Aug. 16, 2018) (notice of action pursuant to Section 301).

30 *Id.*

31 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 47,974 (USTR Sept. 21, 2018) (notice of modification of Section 301 action).

32 *Id.*

33 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (84 Fed. Reg. 21,892 (USTR May 15, 2019) (implementing modification of Section 301 action);

including certain apparel and footwear.[34] These duties went into place on September 1, 2019, at a rate of 15%.[35] The Tranche 4 duties were halved to 7.5% effective February 14, 2020.[36] Since then, no additional tranches of duties have been imposed; nor have any of the existing tranches been modified.

IV. Historical and Recent Trends in U.S. Imports from Hong Kong

Since 1990, U.S. imports from Hong Kong have remained under $12 billion each year. By comparison, the value of imports from china in January of this year alone was more than $39 billion.[37]

During the 1990s, the annual value of U.S. imports from Hong Kong rose gradually, from just under $10 billion in 1990 to a highwater mark of just under $11.5 billion in 2000, the year before China joined the World Trade Organization.[38] From 2001 through 2008, import volumes from Hong Kong fell gradually from $10.5 billion to $6.5 billion.[39] In 2009, as the global recession deepened, imports into the United States from Hong Kong fell to $3.6 billion.[40] From 2010 – 2017, as the effects of the recession diminished, they gradually returned to pre-precession levels, rising to $7.4 billion in 2017, the year before Section 301 tariffs began to be imposed on goods from China.[41]

Section 301 duties were first imposed on Chinese-origin goods on July 6, 2018, and by September 24, 2018, duties had been imposed on tariff lines accounting for $250 billion

---

China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation (84 Fed. Reg. 20,459 (USTR May 9, 2019) (notice of modification of Section 301 action).

34 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 45,821 (USTR Aug. 30, 2019) (notice of modification of Section 301 action). The fourth tranche covered tariff lines accounting for approximately $300 billion in annual imports from China. However, it was divided into two sub-tranches, Tranche 4A and 4B. Duties were ultimately imposed only on tariff lines included in Tranche 4A. While duties were originally intended to go into effect on Tranche 4B tariff lines on December 15, 2019, the imposition of such tariffs was indefinitely suspended in the wake of "Phase 1" trade agreement between the United States and China. *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (83 Fed. Reg. 69,447 (USTR Dec. 18, 2019) (notice of modification of Section 301 action).

35 *Id.*

36 *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation* (84 Fed. Reg. 3,741 (USTR Jan. 22, 2020) (notice of modification of Section 301 action).

37 U.S. Census Bureau, Trade in Goods with Hong Kong, *available at* https://www.census.gov/foreign-trade/balance/c5820.html; U.S. Census Bureau, Trade in Goods with China, *available at* https://www.census.gov/foreign-trade/balance/c5700.html.

38 U.S. Census Bureau, Trade in Goods with Hong Kong, *available at* https://www.census.gov/foreign-trade/balance/c5820.html.

39 *Id.*

40 *Id.*

41 *Id.*

in annual imports from China.[42] Additional tariff lines were subjected to duties starting on September 1, 2019.[43]

To evaluate the impact of the Section 301 duties on imports into the United States from Hong Kong – and particularly to examine whether Chinese goods may have been re-routed through Hong Kong and subsequently imported into the United States as duty-exempt goods of Hong Kong, I reviewed official import statistics for annual and quarterly imports from Hong Kong from 2016-2020.

The United States' tariff schedule is divided into sections according to the general nature of imported goods, and further divided into tariff chapters, headings, subheadings, etc.[44] Based on a review of import statistics collected by the U.S. International Trade Commission, prior to the imposition of Section 301 tariffs, the vast majority of U.S. imports from Hong Kong consisted of miscellaneous articles (including optical equipment, works of art, furniture, toys, and goods classified in special provisions for articles reimported after export from the United States, etc.),[45] machinery and equipment, and precious metals/jewelry.[46] In 2017, goods in these categories accounted for 86.6% of U.S. imports from Hong Kong.[47] Between 2018-2020, the percentage of U.S. imports from Hong Kong accounted for by goods in these categories grew from 85.7% to 93.9%.[48]

In 2017, U.S. imports from Hong Kong totaled $6.8 billion.[49] In 2018, U.S. imports of Hong Kong fell to just over $6.1 billion.[50] The vast majority of this decrease was due to a decline in imports of precious metals and jewelry, which fell by 11%, from $1.26 billion in 2017 to just under $800,000 in 2018.[51] The year 2019, the first full year in which Section 301 duties were in effect, saw a more precipitous overall drop in imports, from $6.1 billion in 2018 to $4.6 billion.[52] The majority of this year-on-year decrease was

---

42 *See* discussion at 4-5, *supra*.
43 *Id.*
44 Harmonized Tariff Schedule of the United States, *available at* https://hts.usitc.gov/current.
45 A substantial percentage of U.S. imports from Hong Kong of "miscellaneous" items enter under tariff line 9801.00.10, applicable to U.S.-origin articles and previously-imported articles exported and then returned without being advanced in value. $2.2 billion in such products entered the United States in 2016. In 2018, the year in which Section 301 duties started to take hold on goods of China, the level of imports from Hong Kong under this tariff line equaled $2.5 billion. By 2020, the number fell to $1.2 billion. U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff heading 9801 and tariff line 9801.00.10, 2016-2021.
46 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong, 2016-2021.
47 *Id.*
48 *Id.*
49 *Id.*
50 *Id.*
51 *Id.*
52 *Id.*

attributable to a steep decline in imports of machinery and equipment, from $1.3 billion in 2018 to less than $600,000 in 2019.[53]

2020 was notable for a spike in imports from Hong Kong. Overall import value rose from $4.6 billion in 2019 to $7.9 billion in 2020, an amount higher than any year since 2006.[54] Nearly all of this increase was attributable to a sudden jump in imports of precious metal and jewelry.[55] Nearly $5.5 billion in precious metal and jewelry entered the United States from Hong Kong in 2020.[56] Notably, the vast majority of these imports entered the United States in just two months – April and May of 2020.[57]

Looking closer at this import spike, the importers were clustered in just two tariff headings, 7115 and 7108.[58] These cover articles of precious metal or metal clad with precious metal (heading 7115) and gold, including platinum-plated gold, in unwrought or semi-manufactured forms.[59] These headings would cover, for example, gold or silver bars, blanks for gold coins, or gold flakes. The vast majority of these imports ($5.2 billion), entered the United States through the Port of New York.[60]

After spiking in the second quarter of 2020, imports under these tariff headings, and under tariff codes generally applicable to precious metals and jewelry, fell back to levels consistent with prior years' quarterly import levels, of approximately $165 million - $300 million per quarter.[61]

To put these figures into context, U.S. imports of goods under headings 7115 and 7108 increased from all countries increased significantly starting in March of 2020.[62] In January of 2020, total U.S. imports under these headings were approximately $800 million.[63] In March, this rose to $4.3 billion, and peaked at $14.8 billion in June of 2018.[64] U.S. imports of gold have remained elevated, compared to historical levels,

---

53 *Id.*
54 *Id.*
55 *Id.*
56 *Id.*
57 *Id.*
58 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff chapter 71, 2016-2021.
59 Chapter 71, Harmonized Tariff Schedule of the United States, *available at* https://hts.usitc.gov/current.
60 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff chapter 71, 2016-2021.
61 *Id.*
62 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption under tariff chapter 71, 2016-2021.
63 *Id.*
64 *Id.*

since the global coronavirus took hold.[65] This is not surprising, given that imports of gold tend to increase during times of economic uncertainty.

During March-June of 2020, imports of gold spiked not just from Hong Kong, but from other territories known as financial and banking hubs, like Switzerland and Switzerland. For example, imports into the United States from Switzerland under tariff headings 7108 and 7115 rose from $67 million in January 2020 to nearly $8.5 billion in May of 2020.[66] Imports into the United States from Singapore under the same tariff headings rose from $1.3 million in January 2020 to $1.4 billion in May 2020.[67]

From January-June 2021, the value of U.S. imports from Hong Kong equaled $1.8. billion.[68] On an annualized basis, imports in 2021 are projected to be lower than in at any time since 2009, when they equaled $3.6 billion.[69]

V. Hong Kong and Transshipment of Chinese Goods

With the imposition of Section 301 duties on Chinese goods, companies importing Chinese-origin goods had an incentive to take actions to avoid the impact of the duties. Some of these actions were fully legal – such as moving production operations, in whole or in part, outside of China, so that their goods would no longer have Chinese origin under the test used by U.S. CBP to determine origin for duty purposes.[70]

However, shifts in trade flows, as well as customs inspections, indicate that certain Chinese exporters, and/or the importers of their goods into the United States, have engaged in unlawful means of avoiding duties.[71] One common scheme for avoiding increased duties on goods of a specific country is transshipment. In a transshipment

---

65 *Id.*

66 *Id.*

67 *Id.*

68 U U.S. Census Bureau, Trade in Goods with Hong Kong, *available at* https://www.census.gov/foreign-trade/balance/c5820.html.

69 *Id.*

70 This test, known as the "substantial transformation test," was developed by the federal courts in the wake of Congress's enactment of 19 U.S.C. § 1304, the federal origin marking statute. The test defines origin based on the last country in which a product underwent a "substantial transformation" prior to importation, and defines a substantial transformation as occurring "when an article emerges from a manufacturing process with a name, character, and use that differs from the original material subjected to the processing." *See United States v. Gibson-Thomsen Co.*, 27 C.C.P.A. 267 (C.A.D. 98) (1940). There, the Court of Customs and Patent Appeals found that "{a} substantial transformation occurs when an article emerges from a manufacturing process with a name, character, and use that differs from the original material subjected to the processing." In practice, the test is highly fact-specific and often requires in-depth analysis of components and manufacturing processes.

71 *See, e.g.,* Chuin-Wei Yap, "American Tariffs on China re Being Blunted by Trade Cheats," *The Wall Street Journal* (June 26, 2019); "Vietnam to crack down on Chinese goods relabeled to beat U.S. tariffs," *Reuters* (June 10, 2019).

operation, goods are routed through a third country so as to disguise their true origin. In the third country, they are generally relabeled or repacked with markings that indicate that they were produced there, rather than in the actual country of manufacture.

To the extent that Chinese companies chose to use Hong Kong as a transshipment hub for evading Section 301 duties, one would expect increased exports from Hong Kong coinciding with the imposition of Section 301 duties on particular product lines. For example, one might expect to see increased exports of machinery from Hong Kong in the third and fourth quarters of 2018, concurrently with the imposition of the first three tranches of Section 301 duties. However, U.S. imports of machinery from Hong Kong grew by only 2% from 2017-2018; the value of imports in this category fell sharply in 2019 from 2018 levels and remain depressed.[72] Even when one considers machinery imports at a more granular level (for example, by reviewing imports of goods under the individual four-digit tariff headings of Chapters 84 and 85), the tariff headings do not reveal substantial increases after Section 301 duties were put into effect. Rather, the trend even at this level is one of substantial declines in imports, particularly between 2018-2019, and into 2020.[73]

For example, in 2018, the United States imported $109 million in goods from Hong Kong of tariff heading 8471, covering automatic data processing machines (computers) and parts thereof.[74] This fell to $53 million in 2019, and $31 million in 2020.[75] Likewise, in 2018, the United States imported from Hong Kong $335 million in goods of tariff heading 8517, covering telephones (including cell/smartphones) and communication equipment such as routers and certain Bluetooth devices.[76] In 2020, this fell to $175 million.[77]

The lack of import growth suggests that China did not turn to Hong Kong as a transshipment hub for machinery,[78] but the severe drop-off in imports is harder to explain. After all, machinery produced in Hong Kong was, and remains, legitimately free of Section 301 duty liability. One possibility might be that while China did not seek to

---

72 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff chapters 84 and 85, 2016-2021.

73 *Id.*

74 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff heading 8471, 2016-2021.

75 *Id.*

76 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Hong Kong under tariff heading 8517, 2016-2021.

77 *Id.*

78 It also suggests that U.S. importers did not turn to Hong Kong as a place to legitimately move certain manufacturing operations so that the resulting products would be considered Hong Kong products under U.S. law. This may have been due to a lack of available capacity there, or because the imposition of Section 301 duties on Chinese goods led certain importers to be wary of production operations conducted anywhere under China's control.

use Hong Kong as a specific transshipment hub after the imposition of the Section 301 duties, the imposition of the duties led importers to realize that goods that they had previously imported as products of Hong Kong were actually of Chinese origin, and to reduce their import volumes accordingly.

Prior to the imposition of Section 301 duties, there were generally no duty differences between goods of Hong Kong and goods of China. This mean that, at least from a duty savings perspective, there was no reason to improperly import Chinese goods as goods of Hong Kong. This lack of duty risk may have led certain importers to pay less attention to the manufacturing processes and locations for their goods than would be ideal. Imposition of duties on Chinese products, however, provided importers with good reason to inquire closely into the manufacturing location of goods purchased from Hong Kong sellers, and otherwise to conduct the detailed, fact-specific analyses required to determine origin under the substantial transformation test. The results of these inquiries and analyses may have led importers to reduce imports, or otherwise to shift their sourcing patterns.[79]

VI. Recommendations

While the import data that I have reviewed does not appear to reflect increased transshipment through Hong Kong in the wake of the Section 301 duties, the territory was a known transshipment hub in the past – particularly for textiles.[80] And transshipment of Chinese-origin goods to avoid Section 301 duties, as well as antidumping and countervailing duties, is a significant problem in countries like Vietnam.[81] Indeed, U.S. imports from Vietnam grew by 26.5% from 2018-2019, and grew by an additional 20.9% in 2020, despite the trade-depressing effects of the

[79] The volume of U.S. goods imported from China did not fall immediately in the wake of the imposition of Section 301 duties. Indeed, by value, imports from China in the fourth quarter of 2018, when the first three tranches of Section 301 duties were newly in effect, increased slightly from $141 billion in fourth quarter 2017 to just over $144 billion. In 2019, imports from China fell significantly from 2018 levels, from $538 billion to $450 billion, a level slightly lower than the $462 billion in imports seen in 2016. *See* U.S. Census Bureau, Trade in Goods with China, *available at* https://www.census.gov/foreign-trade/balance/c5700.html.

[80] *See, e.g.,* Patrick Conway, "How transshipment may undercut Trump's tariffs," The Conversation (Apr. 26, 2018); "U.S. Customs Lists Textile Transshipment, Origin Rule Violators," American Shipper (Oct. 10, 2001).

[81] *See, e.g.,* U.S. Customs & Border Protection, Notice of Action in EAPA Investigation 7250 (Aug. 10, 2021); Chuin-Wei Yap, "American Tariffs on China re Being Blunted by Trade Cheats," *The Wall Street Journal* (June 26, 2019); "Prak Chan Thul, "U.S. fines firms transhipping via Cambodia to dodge Trump's China tariffs," Reuters (June 19, 2019); "Vietnam to crack down on Chinese goods relabeled to beat U.S. tariffs," *Reuters* (June 10, 2019).

coronavirus pandemic.[82] In the first six months of 2021, imports from Vietnam have grown by 46% compared with the same period in 2020.[83]

Vietnam is far from alone in this regard. Trade data also shows significant growth in imports declared as originating in countries such as Thailand, Malaysia, and Taiwan, even as imports from China have fallen.[84] Some of this increase is likely due to lawful trade shifts, with companies moving meaningful aspects of their production operations out of China. But so long as duty differences exist between products produced in different countries, unscrupulous companies will have an incentive for unlawful duty evasion.

To combat transshipment and related practices both today and in the future, the United States should consider several actions, all of which would require Congressional action.

First, CBP should receive increased funding for investigating and addressing transshipment. CBP already has the authority to investigate transshipment and to penalize importers of transshipped goods under 19 U.S.C. § 1592(d), the general customs fraud statute. However, limited resources mean that the agency must triage its enforcement activities. Transshipment is a substantial enough problem to deserve additional, specific funding.

The United States should also consider expanding the reach of the Enforce and Protect Act, or EAPA. Passed as part of the Trade Facilitation and Trade Enforcement Act of 2015, EAPA authorized provided CBP with enhanced authority to combat the evasion of antidumping and countervailing duties.[85] Since the law's enactment, CBP has conducted more than 130 investigations into evasion of antidumping and countervailing duties, and identified more than $600 million in duties owed.[86] Notably, many EAPA investigations involve transshipment of Chinese goods through third countries.[87]

---

82 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Vietnam, 2016-2021.

83 *Id.*

84 U.S. International Trade Commission, Dataweb, U.S. Imports for Consumption from Malaysia, Taiwan, and Thailand, 2016-2021.

85 Trade Facilitation and Trade Enforcement Act of 2015, Public Law 114-125 (Feb. 24, 2016), Title IV, Sec. 421.

86 U.S. Customs & Border Protection, "Enforce and Protect Act (EAPA"), *available at* https://www.cbp.gov/trade/trade-enforcement/tftea/eapa.

87 *See, e.g.,* U.S. Customs & Border Protection, Notice of Action in EAPA Investigation 7250 (Aug. 10, 2021 (Chinese diamond sawblades transshipped through Thailand; U.S. Customs & Border Protection, Notice of Action in EAPA Investigation 7430 (Feb. 23, 2021) (Chinese activated carbon transshipped through Indonesia); Notice of Action in EAPA Investigation 7379 (Sept. 23, 2020) (Chinese wire garment hangers transshipped through India); Notice of Action in EAPA Investigation 7430 (Mar. 9, 2020) (Chinese xanthan gum transshipped through India); Notice of Action in EAPA Investigation 7270 (Sept. 25, 2019) (Chinese glycine transshipped through Thailand); Notice of Action in EAPA Investigation

CBP's successful use of EAPA to combat transshipment in the antidumping and countervailing duty context indicates that the EAPA process could be successfully used to combat evasion of other kinds of special duties, such as Section 301 duties. The process's timelines ensure that action is taken where information available to CBP reasonably suggests that transshipment is taking place.[88] This, in turn, allows the agency to quickly shut down illegal and distortive transshipment operations, and to collect lawful duties on goods previously imported through transshipment. The EAPA process also provides enhanced public visibility into the identities of bad actors, and complicates their ability to simply alter, rather than halt, their transshipment schemes.

Finally, the United States should consider enacting a statute similar to 19 U.S.C. § 1592a, a statute passed in the early 1990s, at a time when the United States still maintained a country-specific quotas on imports.[89] Among other things, this statutory provision requires CBP to publish, at least twice a year, the names of foreign entities and persons who have been issued penalties under the agency's general fraud statute for "engaging in practices which aid or abed the transshipment, through a country other than the country of origin" of textile products.[90] The statute also places a heightened requirement of "reasonable care" on importers that enter goods supplied by such persons or entities.

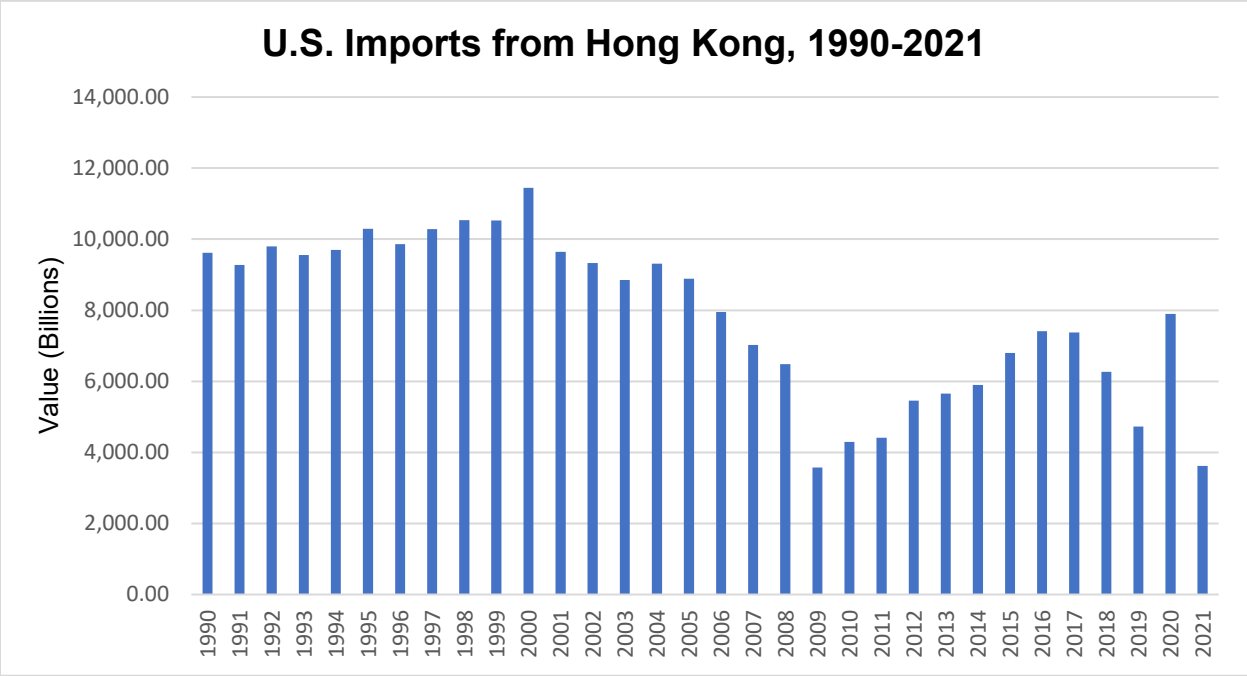
While 19 U.S.C. § 1592a applies only to transshipped textile products, it provides a model that could be used with respect to transshipment more broadly. Public naming and shaming of bad actors would bring heightened visibility to the problem of transshipment in the trade community. It would also provide useful information to importers that might otherwise believe that they were legitimately purchasing non-Chinese-origin goods.

7232 (Mar. 20, 2019) (Chinese aluminum products transshipped through Vietnam); Notice of Action in EAPA Investigation 7191 (Mar. 15, 2018) (Chinese wire garment hangers transshipped through Malaysia).

88 19 U.S.C. § 1517.

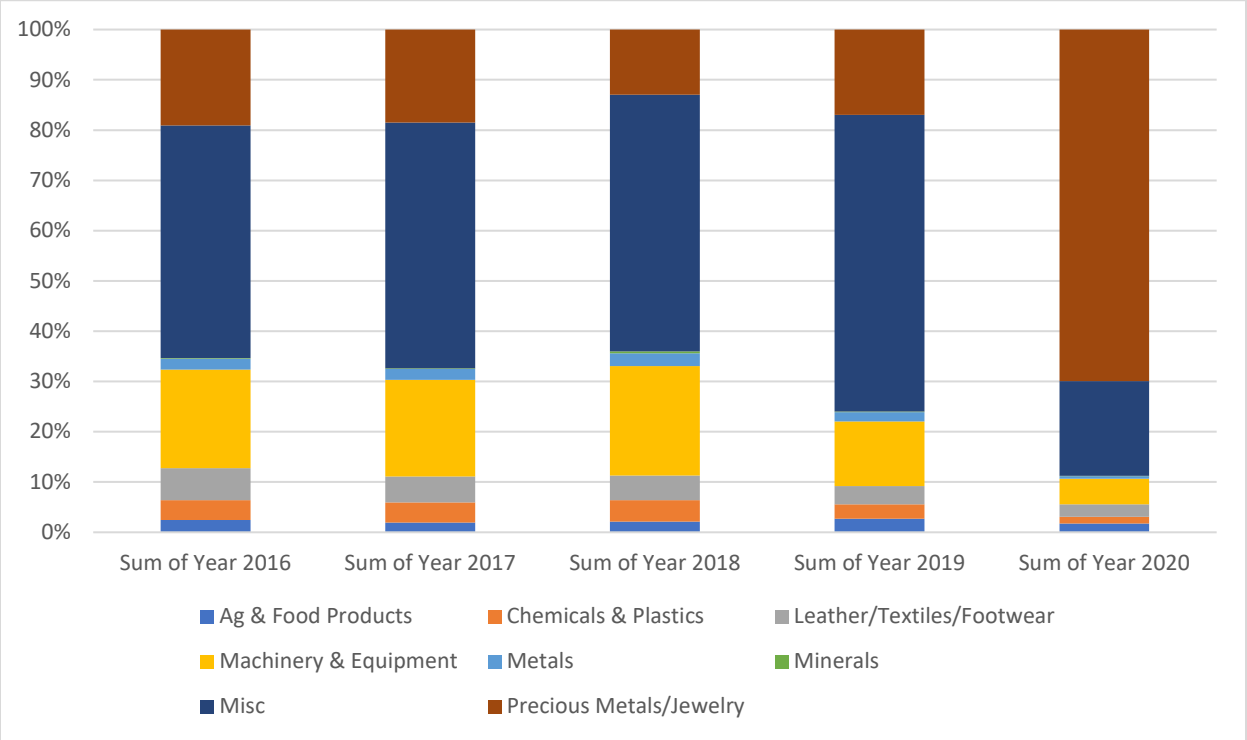
89 The United States fully removed this quota system in 2005.

90 19 U.S.C. § 1592a.



Source: U.S. Census Bureau, Trade in Goods with Hong Kong[91]

Relative Percentage of U.S. Imports from Hong Kong by Product Category, 2016-2020



Source: U.S. International Trade Commission, Dataweb

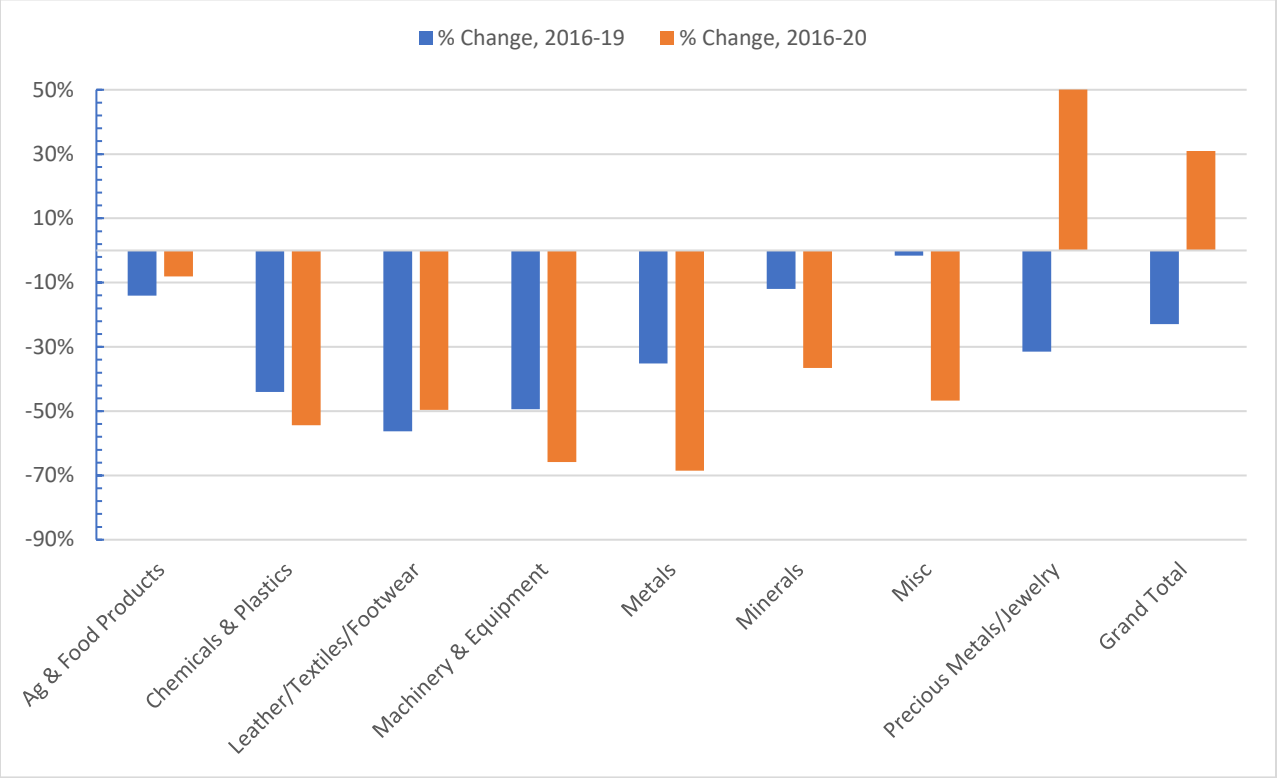
[91] 2021 data have been annualized. From January-June 2021, U.S. import from Hong Kong were $1.8. billion.

Year-on-Year Change in Value of Imports from Hong Kong by Product Category

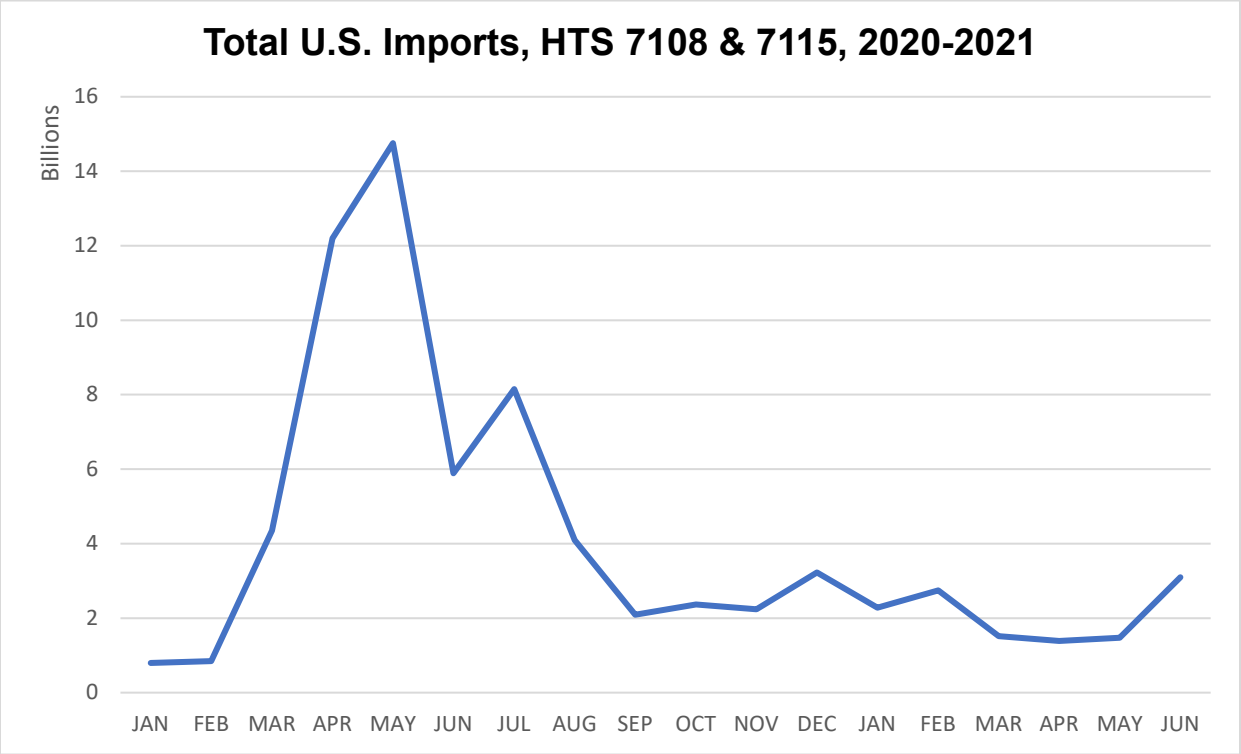
	16-17	17-18	18-19	19-20
Ag & Food Products	-11%	2%	-5%	7%
Chemicals & Plastics	17%	-5%	-50%	-18%
Leather/Textiles/Footwear	-8%	-14%	-45%	15%
Machinery & Equipment	12%	2%	-56%	-32%
Metals	11%	9%	-46%	-51%
Minerals	97%	80%	-75%	-28%
Misc	20%	-6%	-13%	-46%
Precious Metals/Jewelry	11%	-37%	-2%	600%
All	14%	-10%	-25%	70%

Source: U.S. International Trade Commission, Dataweb

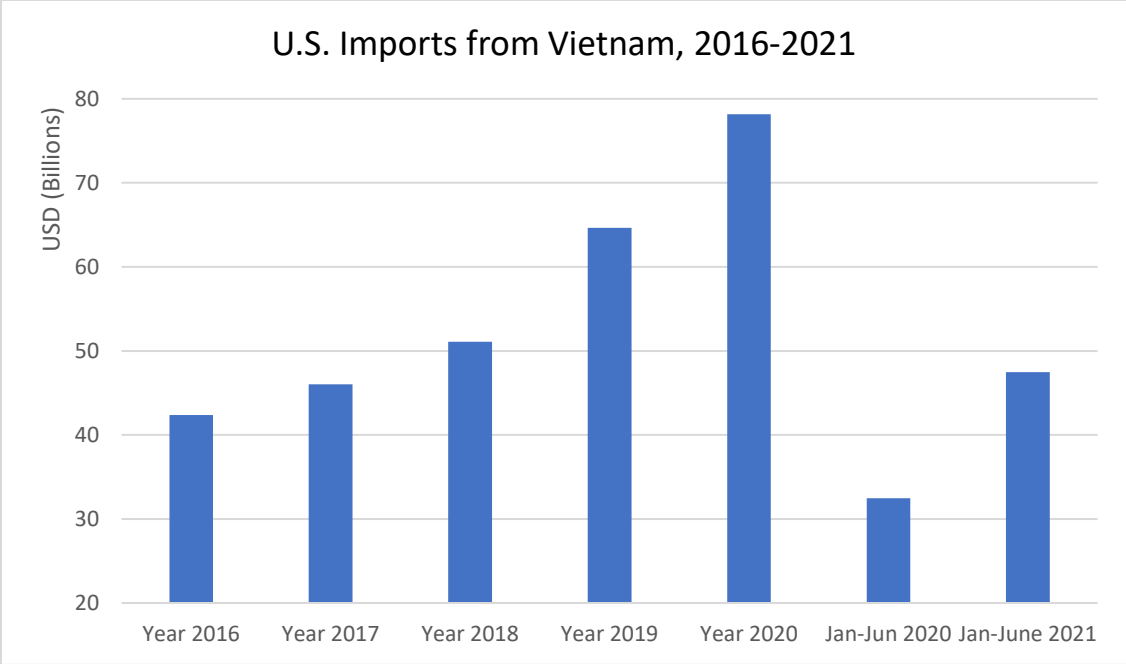
Change in Value of Imports from Hong Kong by Product Category, 2016-2020



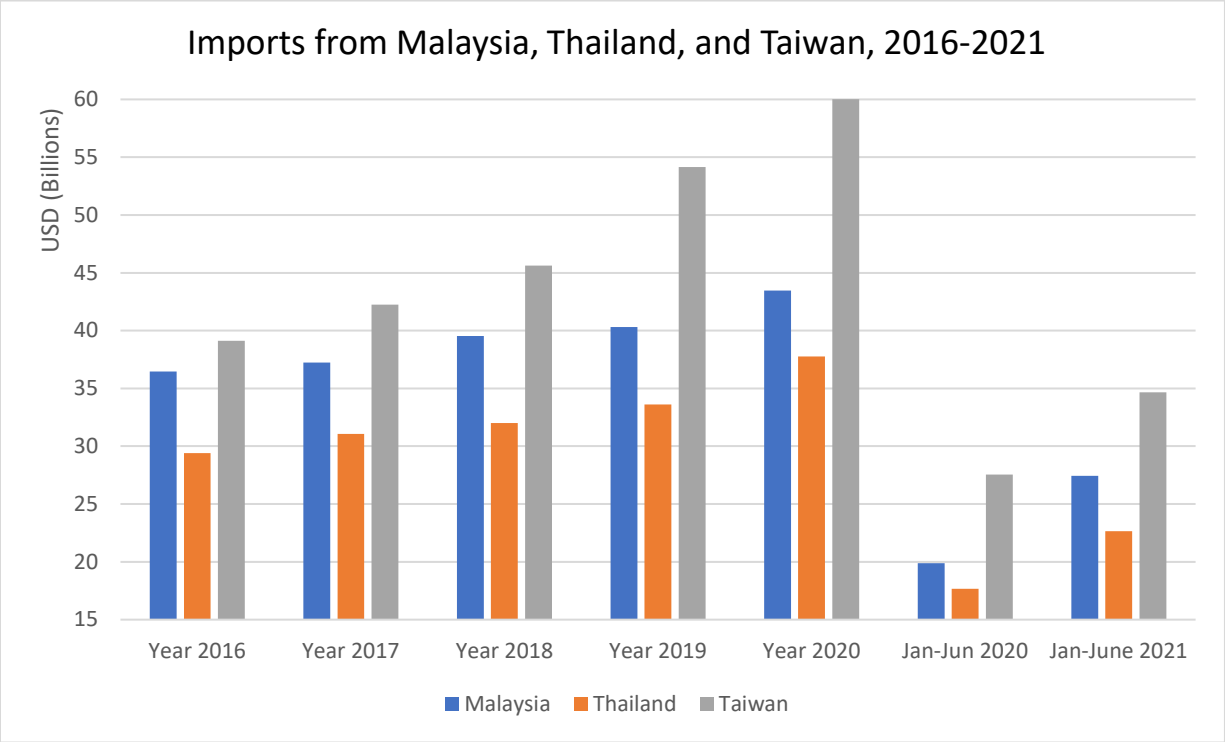
Source: U.S. International Trade Commission, Dataweb



Source: U.S. International Trade Commission, Dataweb



Source: U.S. International Trade Commission, Dataweb



Source: U.S. International Trade Commission, Dataweb

PANEL I QUESTION AND ANSWER

VICE CHAIRMAN CLEVELAND: Thank you, Ms. Thorson. Chairman Bartholomew, we'll start with you with questions.

CHAIRMAN BARTHOLOMEW: Yes, thank you, thank you Vice Chairman Cleveland and Commissioner Glas for pulling together this hearing. It's such a distressing panel, such a distressing situation in Hong Kong. But I really want to commend our witnesses for their continuing work, which comes at some risk to all of them and to their families. So thank you for that. I think one of the first questions I'd like to start with, first is, it's a technical one. And I could be wrong, of course. But when they passed the National Security Law didn't Carrie Lam say that it was prospective? And not retrospective?

MR. DAVIS: Yes. And there's an article in it that says that it should only apply prospectively. It's not retroactive. But we have to bear in mind what they've been doing. And this is how they've been going after organizations, is they look at the organization's track record, like the Alliance that Samuel talked about today. And they say, well, all the things you did before the law was passed shows what your views are. And therefore you still exist. So in effect, we're investigating you. And we'll see what happens. So these organizations know that there's a way that retroactivity sneaks in the back door.

CHAIRMAN BARTHOLOMEW: And thank you. That's just another example of how I think we can't

VICE CHAIRMAN CLEVELAND: Carolyn, I think Ms. Datt had something to say.

CHAIRMAN BARTHOLOMEW: Oh, sorry. Can't it's difficult for us to see everybody. Ms. Datt?

MS. DATT: Sorry, I was just in the media space, too, with Apple Daily, police pointed to some articles that were written before 2020 as examples of how the paper supposedly colluded with foreign forces. So that also is kind of the retroactive nature of how that NSL being used.

CHAIRMAN BARTHOLOMEW: And wasn't there just someone who sang at a campaign event, I think in 2018, or 2019, who was also charged.

MR. DAVIS: Samuel, do you know?

MR. CHU: Yes, I think that, Chairwoman, I think what you're referring to, I think there's actually been a number of incidents or examples of how our time has been warped in Hong Kong. Where Carrie Lam actually went to the U.N. and said it was not retroactive. But for all the legislators who have been disqualified, their disqualification is based mainly on speech, and beliefs, and things that they have actually said prior to the enactment of the National Security Law. So you are correct on that point, is that, it seems like that the National Security is not only retroactive, it's also future proof in this case.

CHAIRMAN BARTHOLOMEW: Thank you. My time is mostly up already. But I wanted to ask if you guys have observations on whether the U.S. business community should be concerned and what the impact on their ability to do business might be with the National Security Law?

MR. DAVIS: The answer to that is clearly, yes. And there was a vote in my statement, my written statement, I mentioned this. The American Chamber of Commerce and 40 percent of the members indicated they were planning to leave Hong Kong. So they are in fact concerned

about it. And now with the threat of an anti-sanction law being enacted locally in Hong Kong, if the businesses engage in activities that they're required to do by U.S. law, then they may be faced with even under this law, on the mainland, involves private lawsuits that can be made. And in fact, companies, mainland companies are obliged to do this. It's a form of getting them to report on any kind of deal problems they have, where U.S. companies may be following their sanctions regime. So it's a very serious problem for U.S. companies.

MR. CHU: And I'll just note that, Chairwoman, that this past weekend, the whole outside, independent, Board of Directors of Next Digital, the media company that owned Apple Daily and is owned by Mr. Lai, have voted to They all resigned and asked that they could no longer function. And so, they are liquidating. They're hoping to liquidate the resources and be able to pay former staff and investors. That will happen and will continue to happen. And I believe that that is a warning sign to everyone who's doing business in Hong Kong.

CHAIRMAN BARTHOLOMEW: You know, it's interesting with Apple Daily, of course, that what is it? It's illegal not to pay your employees in Hong Kong. And yet, when Apple Daily's assets were frozen, they were put in the position of actually violating the law, even though they were trying not to do that.

So I've been just, I guess, surprised or shocked that people in the U.S. business communities somehow think that they are safe from all of this. You know, they look at Jimmy Lai, and they say, well, he was doing that, and we're not doing that stuff. But I think it's important for people to continue to focus on the risks that they'll all be facing. With that, I think my time is up, we'll move on to the next person. Thank you. Thanks, again, to our witnesses, and for all the work that you do.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Borochoff?

COMMISSIONER BOROCHOFF: You said you were speechless after listening to Mr. Chu. And I want to say thank you to this group. You've done just a phenomenal job of displaying exactly what's happening over there with this.

I would call it a national subversion law, because it really is subverting the values of this civil society, at the same time, that it allows people to be accused of any kind of, even the inference that they are subverting this groupthink that's being forced on that society. It's more than alarming. And it's frustrating to me that, that not everyone in America really understands it. So this is an important testimony that you all are giving.

It's not often that, that I listened to lawyers testify and they're so engaging. So I want to thank the two lawyers who spoke on this testimony today. It really, it was I learned a lot from reading everyone's written testimony. I would characterize to say that, that you all, particularly, the two attorneys, Ms. Thorson, and Mr. Davis did a great job of describing what's happening over there. Ms. Datt, particularly interested in and I would like all of you after she answers this to tell me if there is a way.

You talk about in your written testimony that we need to, and I just want to quote it, "divert internal resources of technology companies to protect internet freedom in Hong Kong." So I have the question, specifically what you meant by that? And then, do any of you think that's even possible, based on what's happening. Clearly, the internet is being used as a weapon everywhere, including in America. The question is, are they removing that ability completely? And is there a way to protect the media or even influence the media, today, forward?

MS. DATT: Thank you for your question. So that specific recommendation is related partially to something that Facebook did in relation with Taiwan's presidential election. Where they set up what they call the war room, to coordinate different offices to respond to this information. So I think the technology companies have the finances and the ability to set up, maybe, some more specialized and targeted responses.

It was clear that there was a large Chinese backed disinformation campaign in that election. We don't see anything like that. We don't really see any statements or proactive action from them about Hong Kong. And it's clear that, you know, digital rights are eroding in Hong Kong, the Hong Kong Police ordered a website to be taken down globally after it sent a letter to the Israeli hosting company. So it's, also, you know, our ability, people outside of Hong Kong to access information.

So I had some recommendations in my written testimony. But I think technology companies, which dominantly predominantly are American, there's a lot more that they can do, just by coming to the table addressing the fact that this is happening, and not kind of trying to hide.

COMMISSIONER BOROCHOFF: So you're talking about them broadcasting this to the world rather than inside Hong Kong?

MS. DATT: Yes, both. Because when the National Security Law came into effect, a lot of the company said that they would no longer comply with police requests for user information. But that doesn't address takedown requests, which is a very nice way of saying censorship. And there's also not a lot of transparency from the companies when they get these requests. And we've seen, at least with mainland China, say like a company like Apple is taking action, sometimes internally without even a government request to remove apps or content. And so I think that, yes, these companies need to both broadcast globally that they're, you know, they will defend digital rights, partially because by enforcing some local laws, they might be complicit in human rights violations, and might be subject to sanctions from democratic countries. And now with the Anti Sanctions Law, they might be subject to Chinese sanctions for enforcing other sanctions. So I think companies can't really sit on the sidelines anymore.

MR. CHU: If I can add, I think based on some of our internal research over the early part of this year, I think that the Hong Kongers are generally more aware of censorship, or when websites are blocked. Because they have had the internet free access for you know, decades, and then, years and years. I equated to kind of like telling your kids that the TV doesn't exist. And it does allow for an opportunity to do some preemptive work of training as far as internet security. And for the U.S. and other international community to provide some digital training. And as we can see that there are still ways to get around, even the great firewall. But we have to do those tools and training, now, rather than later. A heightened awareness, as we found out from Hong Kongers, about internet censorship does not make them any more equipped to overcome the barriers. And then, I think one big note that I would say is that, I think it is really important for the U.S. to set out our own version of digital democracy in order for the world to be able to follow and to be modeled after. Because that's what the Chinese government are doing. They are modeling and exporting digital authoritarianism, through all means and ways around the world. And that, we have to counter that by setting up our own model and be able to share that across the globe.

COMMISSIONER BOROCHOFF: You know, Mr. Chu, you're out of date, because for most kids TV doesn't exist today. Which, what you need, you need update and say Amazon Prime doesn't exist or streaming doesn't exist.

MR. CHU: Or your smartphone, your phone doesn't exist.

COMMISSIONER BOROCHOFF: Right, exactly. But the points well taken. Sorry to interrupt.

MR. DAVIS: I would add that there's another form of software, if you will, and that's universities and the pressure on universities in Hong Kong, I think is really great now. It's interesting to me because as someone who's coming and going for, in recent years, I would, I'd find that now reporters call me every week because the professors in the universities that used to be a resource can't speak anymore. They're afraid to speak. They're under pressure. And this, I think, has a profound impact. I worked at two of Hong Kong's universities, the Chinese University of Hong Kong, and then, later the University of Hong Kong. And they're both ranked among the top in the world. So the loss for, you know, education in Asia of research, and so on, if these universities are degraded, is enormous. And I think it's something, also, that we should be paying attention to.

Right now, Hong Kong is still outside of the Chinese firewall. So professors doing research and stuff can go ahead and get access to information as universities do here. But I think if the internet is closed down, or shut down, or soft, or things are not available anymore, then the impact will be quite large in Hong Kong. I think it will change the very character of the society.

VICE CHAIRMAN CLEVELAND: It will add to changing the character of society.

MR. DAVIS: Yes.

VICE CHAIRMAN CLEVELAND: But yes, I'm sure of that

COMMISSIONER BOROCHOFF: Thank you.

VICE CHAIRMAN CLEVELAND: that view. Thank you, Mr. Borochoff. Commissioner Fiedler?

COMMISSIONER FIEDLER: Yes, thank you. Let me ask a question about what exists to inhibit the Chinese government from trying people in Chinese courts and incarcerating them in Chinese prisons in Hong Kong?

MR. DAVIS: The answer is nothing. The National Security Law has provisions that allows cases to be removed. In the Jimmy Lai bail case, there was actually an implied threat published in the People's Daily that seemed to suggest that if the court, the Court of Final Appeal didn't rule the way Beijing wanted it to, that they had the option to move the case. And the people who would decide that is that office I mentioned earlier, the Office for Safeguarding National Security, which is staffed entirely by mainland public and State security officials, not Hong Kong officials.

And it says in the law that the Chief Executive has to approve it. But I think that's kind of pro forma because the Chief Executive seems now to approve everything that the China wants to do. So I think the threat is actually on the table and may still be there in the Jimmy Lai case. Yes, there's some sense I got, as they went after some leading figures who had not been advocating any violence or anything in the protest, that there was some score settling going on. And some of these people like Jimmy Lai, Martin Lee, Lee Cheuk-yan, and others, I think they really wanted to get them. So if the Hong Kong laws somehow protected them, then I think the

risk of their removal would be very high.

MR. CHU: And I would add that I think that this is a clearly a case of where they are doing a serial prosecution. Where, almost everybody who has been convicted, or are currently in prison, has been convicted, again, multiple times while they're in prison. So I think they're working their way through the ladder of what they can do, and with the intention of really detaining them indefinitely. I do want to point out that there were 12 activists who tried to escape Hong Kong to Taiwan in a boat. They were captured a year ago by Chinese Coast Guard. And they were tried in the mainland. And were convicted of essentially illegal crossing, which in itself is an interesting issue to the debate of where they were crossing from where to where. But I think that what, you know, Professor Davis also said, the courtroom environment in Hong Kong are now essentially in a lot of ways similar to the environment in China.

Just this morning, Chow Hang-tung, the barrister and the Vice Chair for the Alliance was arrested, she was serving as the lawyer for one of the 47 candidates who ran in the primaries who were all arrested and charge. Gwyneth Ho, one of her clients was due in court this morning. And had her lawyer, essentially, removed, arrested herself. And Gwyneth, in her application, talks about the reality of why she was choosing to stay in jail because she was rejecting the idea that her bail hearing would be a closed door affair rather than a regular hearings.

COMMISSIONER FIEDLER: Samuel, let me follow up asking you what would the impact in Hong Kong be if someone was moved to Chinese prison to serve out their sentence?

MR. CHU: Yes. I think that as Professor Davis talked about, I think the Jimmy Lai case is probably the one that many had feared that would be the test case of actual extradition. I think that the impact is already, has already arrived because the threat of it is what I think makes a difference. I think that the idea of individuals prosecuted for speech, and for political views, is the reason why I think that the white terror atmosphere. And the threat of actually not receiving any kind of open and fair trial, and a 99 percent conviction rate, and many others who are still imprisoned in China, without access to any outside connections, or counsels, I think the threat of that already exists and already has an impact in Hong Kong.

MR. DAVIS: I would add here that if they are transferred to the Mainland, the National Security Law provides that mainland procedures will be applied, not Hong Kong trial procedures in any form. So whatever kind of trial one would expect, for this kind of charge on the mainland, is what the defendant would get.

COMMISSIONER FIEDLER: Thank you, very much. If you have time to stick around, I'll be here.

VICE CHAIRMAN CLEVELAND: Okay, thank you. We might ask for the record for a little more detail on that very distinction, Mr. Davis, between mainland procedures versus. But I don't think we'll get into them here today. So, Commissioner Glas?

COMMISSIONER GLAS: Thank you, Vice Chairwoman. I want to thank all our panelists. This has been an incredible panel and I could spend hours with probably each of you to talk about these very complicated issues. I do have a couple questions related to internet censorship, and what you're seeing in Hong Kong, and what the likelihood is that internet censorship will mirror what's happening in China, and what are the economic trade and security implications, if in fact, Hong Kong's internet censorship, the mirrors that of China?

And then, the other question I have is actually directed to Ms. Thorson and your testimony. You know, I know at that end of the Trump administration, there were changes made with the designation of Hong Kong products, i.e. being Chinese goods. But what difficulties exist in determining the origin of transship goods that things are actually made in Hong Kong? So this is a two part question. I think the other question might be better directed at some of the other panelists. And then, Ms. Thorson at the very end.

MS. DATT: Well, I'll start on internet censorship. Right now, the internet censorship system is not the same, but it is likely going to move in that direction as mainland China's. But I think they're, we're still far from that point. Because as I mentioned, Hong Kongers grew up with a free internet. You know, Facebook, Twitter, there's still unblocked.

They're still channels that people use. So, you know, if those web sites were to be blocked, I think that would be a first indication of the deterioration of internet freedom in Hong Kong to the point where we're getting closer to the mainland. And I think Samuel's testimony really pointed out, right now, the police are really concentrating on cracking down on the ground, on a freedom of assembly, on people gathering, on civil society groups organizing.

And, you know, to kind of take the opposition activists off the ground before going to the internet space. So currently, you know, there are no media websites that are blocked in Hong Kong. That would be a warning signal of deterioration. And, you know, the increase in any kind of censorship would be detrimental to both the Hong Kong people, and any business, or entity operating there because it restricts the flow of information. And you know, free flow of information is fundamental to doing business.

COMMISSIONER GLAS: Thank you. Anyone want to follow up on Ms. Datt's points before turning over to Ms. Thorson?

MR. DAVIS: Well, since you invited, I'll just comment that Hong Kong's economy is really based on information. It's a finance system. Mostly the big money's made in finance. And the other thing that Hong Kong has, as I just mentioned, is universities, education, intellectual property. So if you're confining access to that sorts of information, you've got a problem. I will say that many of us now communicate with our friends in Hong Kong, in encrypted messages, and so on. That this is becoming a norm in Hong Kong because of concern about because under the law, the National Security Law under Article 43, and the regulation set up under it, the police could engage in surveillance of your communication. So this is, there's no privacy protection for it under that law.

COMMISSIONER GLAS: Thank you, Mr. Davis. Ms. Thorson?

MS. THORSON: Thank you. So you've asked a very good question about how practically speaking can one determine whether a good is really from Hong Kong, or produced there, or was produced in China or elsewhere. And this is a difficult area for customs enforcement, because you can't really look at the paperwork. Because the paperwork of course, has been spoofed. And you can't necessarily look at the product itself and tell where it came from. It's packaged to reflect the transshipped country of origin. So what Customs has to do, in many cases, is physically have Customs Officers or Customs Attaches, go to the foreign country where the good is supposed to have been produced, and examine the factory.

Actually go in there, and you know, see all the production equipment, take records, and figure out if the supposed factory where the product was made actually exists, if there's a

building there at all. I have heard of cases where Customs goes and finds a forest, where there is supposed to be a factory. Oftentimes, there might be warehousing, but no machinery, things of that nature.

And a lot of information on this kind of thing has come to light from the Enforce and Protect Act process, which provides a lot more public visibility into the kinds of things that Customs is finding when investigates transshipment, in the anti-dumping and countervailing duty context. But it is frankly a very difficult thing to do to confirm whether goods have in fact been transshipped or not.

COMMISSIONER GLAS: Thank you, Ms. Thorson. I think that provides context to some of the key recommendations that you've made. So I'm over time. So I'm handing it back to Vice Chairwoman Cleveland.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Goodwin?

COMMISSIONER GOODWIN: Thank you, Chair. And my sincere appreciation to the panel for your great testimony today. As a commissioned, resident, intersection lawyer, let me ask kind of a simple legal question. Does National Security Law violate international law? As your testimony details, the developments in Hong Kong over the past year are certainly troubling, as troubling as the Chinese Communist Party's approach to issues of speech in the rule of law in mainland.

But especially concerning here, I think, is as Commissioner Glas noted in her introductory remarks is that the steps taken in Hong Kong appear in total disregard for international obligations. So all countries have some latitude to act in their national security. But does this law violate the Joint Declaration? Does it violate international obligations, including those under the Convention on Civil and Political Rights, which both the Joint Declaration and the Basic Law specify will remain in effect? And does it violate general treaty obligations? And assuming that it does, how what should we do? How does that inform our response and that of our partners, now?

MR. DAVIS: The answer is obviously, yes. It violates international law. It violates the Sino British Joint Declaration because the promises of free speech are offended. We even have a judicial opinion in the Tong Tak Shi case already showing that the promise of international human rights in Article 4 of the NSL is not complied with. The provisions in there setting up mainland offices in Hong Kong, violate the guarantees that Hong Kong would have a high degree of autonomy. You know, the due process, the lack of independence of the courts violate any kinds of standards under international human rights treaties.

And the ICCPR does apply in Hong Kong, regarding the proper processes of law, and so on. I think quite frankly, we've tried and I've written this in my statement. I didn't speak about it yet today. But I think that we've tried some sanctions targeting individuals in Hong Kong. I think that's not been very effective. It makes a nice statement of our views, but it doesn't move them to consider change. So that there has to be, I suppose, if you want to be effective, a more comprehensive approach. That is what I talked about in there.

That the United States, obviously, knows and always has to get his own house in order because if we take unilateral approaches to things like this, then the other side just pushes back. Whataboutism, you know. You guys are just as bad.

So I think if you want to respond to international human rights concerns there, a more

comprehensive approach that involves alliances with other countries and international human rights fundamentals that we are committed to in our laws that we pass. And that our companies or any extension of the United States, in any form, is meant to comply with these international rules and so on. They don't always have to be worded in the language of sanctions, because sanctions just gets a push back, a response. And then, I think the other side of it is to deal with the immediate problem. And that's a kind of, on the immigration track in Hong Kong. I think there's more we could do to receive Hong Kongers, who are fleeing from tyranny. And I think it's a great asset. I've seen reports that 1,000 people a day are leaving. The schools, elementary schools are now not having enough students because people are leaving. So receiving those people

The President, Biden, recently extended Hong Kongers who are in the United States. I think other things can be done. Like Canada has a principle that if Hong Kongers have a Canadian degree, they can come to Canada. So that's a kind of option. I think a lot of Hong Kongers have studied in the United States and have great talents that they've taken back to Hong Kong. But if they can't perform their professions in Hong Kong, and they want to leave, if we can receive them back. Again, that is a response to a kind of human rights thing. That's a very concrete thing that could be worked on in U.S. law. And I think the United States would only benefit from it because we're talking, in that case, about talent. Of course, refugees and asylum, or other things that reach people in all sectors of the society and looking at how we manage that and how efficient it is, is something else I think we could do.

COMMISSIONER GOODWIN: Well, very quickly, with my limited time left, I also wanted to get a quick response to the continued involvement of British and Commonwealth Judges in the Hong Kong judiciary. A statement issued I believe, last week by the President of the U.K. Supreme Court indicated that in their assessment, the judiciary in Hong Kong continue to be independent, and their decisions continue to be consistent with the rule of law. This continued involvement I think by U.K. judges is certainly troubling because I think it lends credence to the changes in their system and the erosions in judicial independence. But equally concerning would be what would happen if they leave? So I just wanted to get your reaction, the panel's reaction to the role of British judges and that recent decision. Lawyer?

MR. DAVIS: I'm a lawyer. Well, you know, of course, you brought up yourself exactly what the problem is. There's a belief, apparently expressed my British judges, that being present is better than not being present. So they they're not quite sure what to do. That, the reason they're there in the first place, we have to understand was an attempt to build confidence in Hong Kong. So that these judges would be there. That the Court of Final Appeal because we're talking about the Court of Final Appeal. There are lots of foreign judges in the lower courts already. They're regular Hong Kong employees, and they live there for years. And they're not outside judges. So we're just talking in your question about the ones who come and sit on the Court of Final Appeal. So there's certainly an advantage for them there to sort of provide oversight on the one hand. And some have quit from, I think, Australia, because they wanted to protest at what's happening. I really -- I think it kind of comes down to their conscience in some ways because it kind of cuts both ways. I hate to see the pressure the court will be under if there are no foreign judges in the Court of Final Appeal anymore. So they certainly I think perform an important function. It's not that the Hong Kong judges are incapable and need foreigners because they're not enough.

There's tons of legal talent in Hong Kong. So we're talking about pressure on the courts. And the pressure now is mounted quite severely. Constant criticisms of the courts. Talk about imposing reforms on the court and so on. And so this, I think, I wish I could give a definitive answer. And I think they certainly struggled with this problem in the U.K.

COMMISSIONER GOODWIN: Thank you.

VICE CHAIRMAN CLEVELAND: I think for the record, Mr. Davis, we might ask to come up with some kind of matrix that provides, perhaps, thresholds of if the court moved in this direction and proceeded to rule on the following, in the following manner, inconsistent with international law, that might be the time to collectively consider no longer supporting foreign judges on the Court. But we'll take that up, perhaps.

MR. DAVIS: I can say, I like your metrics.

VICE CHAIRMAN CLEVELAND: Okay.

MR. DAVIS: That's good.

VICE CHAIRMAN CLEVELAND: I'd like you to give context, perhaps. (Laughter.)

VICE CHAIRMAN CLEVELAND: Because I think that's part of our recommendation process. Right? That it would be helpful. So I think we need to, if we're going to act collectively have some common, common understanding of what the standards are. Sorry, Commissioner Kamphausen.

COMMISSIONER KAMPHAUSEN: Thank you, and thanks to our panel. I'll add my thanks to those of my fellow Commissioners that in the insight and wisdom of your testimony. Keith Richburg is a longtime Washington Post reporter. He's now, I believe, resident in Hong Kong and director of the University of Hong Kong Journalism and Media Studies Centre. He wrote an opinion piece in the Washington Post three days ago. I want to read a couple of quotes from that article. And then, invite your comment. He essentially says, Hong Kong is now a tale of two cities.

One Hong Kong is populated by bankers and financial services professionals, real estate developers and property owners, and businesspersons whose primary pursuit is trade with mainland China. In this universe, times are good and getting better and the National Security Law helps. The other Hong Kong is populated by people in the public space, politicians, journalists, teachers, labor leaders, artists, filmmakers, those active in civil society groups, as well as many students and young people. To them, Hong Kong has become unrecognizable. A place where dissent is crushed and debate stifled. Your testimony today really speaks to the second group. He then quotes an expat businessperson in Hong Kong who says China wants to keep Hong Kong. It just wants to get rid of the Hong Kongers. I'd like to invite your comment on this notion of two cities and the implications of that, even for U.S. responses.

MR. CHU: If I can begin. I want to say that I think we have been here before. We have been sold this idea that you can have the economic freedoms and somehow that will maintain or lead to greater human rights. The U.S. has been sold that story from the beginning. I would say that, I think, to the quote and I think that is an interesting moment in time. Right now, being able to say that. Can the business community, can those bankers, traders who are looking to continue, really trust that the crushing of the civil society and the public space is going to stop when it comes to the line of business, and investment, and finance? And I think that we, I think, from my perspective, know the answer to that, is that, it is not going to. We are seeing a preview of the

closing of Hong Kong. Not just for the future of the public sector, but we're seeing the way in which that the private and investment sectors, and finance and trades are going to be shut down. In fact, the playbook has been written. The script is there and it is unfolding as we speak.

MS. DATT: And yes, to add to that, I think in some sense, Hong Kong has been a tale of two cities for many years. When I lived in Hong Kong, you know, there were the experts and the businesspeople who never really took part or cared about human rights. And at the time, I was working on human rights in China, in Hong Kong, and it was a safe place to do that. But it no longer is. But I think it's very naive of them to think that they would be protected.

When I lived in Hong Kong, a Chinese billionaire was kidnapped from the Four Seasons Hotel. And I think there have been many indications that if the CCP wants you, or will target you, it doesn't matter really, that, you know, there's certain laws to protect you. So I think the National Security Law, the impact on the media, on internet, on civil society, you know a free society has free exchange of ideas and without that, I think nobody's really safe.

MR. DAVIS: I would add that there's, I think, a very important business angle that undermines this Pollyannic view of doing business in Hong Kong. And that is, what do Mainland officials do to businesses in Hong Kong? What do they demand of them? And who is favored when it comes to getting deals in Hong Kong, or even across the border? What companies are likely to be favored? I think when you have this system intruding into Hong Kong, what you have is corruption.

You have people who are friends who are favored. So then, the businesses have to go along to get along. HSBC experienced that pressure on them. Cathay Pacific, likewise, pressure on them to say things supporting the National Security Law, and so on. So if you're either an international business or a local business, someone who belongs to the American Chamber of Commerce, or the general Chamber of Commerce, then you're going to feel pressure to go along with whatever Beijing wants. And if you don't, then you're going to suffer for that. And to me, that's nothing other than pure corruption. And so, I think what has happened in Hong Kong's economy today is it's much more corrupt than it used to be, in a very sort of, at a macro level. It's not the kinds of petty bribes, but it's basically if you want to be a part of the game, then you have to go along with whatever they're demanding of you. And I think this is ignored at Hong Kong's peril.

Because we know companies like Alibaba, Tencent, and others are under pressure on the mainland. There's a very clear sign right now that Xi Jinping is going after large private companies that are thought to be powerful. So what happens in Hong Kong? I guess, is that Li Ka-shing invest all their money abroad, somewhere else, and mainland companies come in. And then, they have to dance to the tune that they're given. And I think this is the problem with it. There is an element of truth. I read the article you're talking about. There's an element of truth to the divided society, but perhaps not enough thought about the consequence.

VICE CHAIRMAN CLEVELAND: Our last trip to Hong Kong, we heard a good bit about that, that pressure that you're describing. And it's interesting to me that the extradition treaty seemed to focus the business community's attention two years ago. And I think what happened next caused them to retreat somewhat. Senator Talent?

COMMISSIONER TALENT: Already. You know, we have to make recommendations to the Congress. What do you all think about recommending that they create a new Assistant

Secretary of State for a Hong Kong Bureau? And the only thing this new, Senate confirmed, this new official with a budget and his staff would do is tell the world what's going on in Hong Kong. Is publicize it. Because you know, they did this to the Tibetans. They did it to the Uyghurs. They're doing it to the Mongolians. But this is Hong Kong. And we have a lot not that it was right what they were doing to them.

The point is, this is a very well-known public place with a very heavily developed civil society, with a lot of people like you, Mr. Chu, and you, Ms. Datt, and you, Mr., who are who are perfectly willing, I would expect, to be willing to tell the world what's going on, and what the community of common destiny really means for people around the world. I think they may have made a mistake here, from their own perspective, if we take advantage of it. So what do you all think about a recommendation like that? And by the way, I think Congress can provide.

The new Assistant Secretary would have to be somebody with personal experience with the dissident movement, or dissident affairs, or something like that. That's probably who the President would appoint anyway. But the point is, somebody who really knows this and will be motivated to do something about.

MR. CHU: So I can begin. First of all, I think that I would much rather the bipartisan leadership continue in Congress to actually be the face of the voice and the Administration, from the President, down to the Secretary of State, continue to actually speak specifically on Hong Kong. Because I think that that has been one of the most effective tools that the U.S. has deployed. On an organizational level, I think on the Agency level, I believe that there are coordination beyond just the, you know, speaking out that actually are needed.

Professor Davis talked about the sanction schemes and ways in which that not, just the way, you know, with sanctions. But also, the proactive programs, across Agencies, needs coordination. And that role I think needs to happen and be reconstituted. There used to be a inter Agency working group on civil society and democracies that existed. There used to be a Senior Advisor for Civil Society and Democracy within the State Department. That needs to be reconstituted. But I think that I want to make sure that the role is not just about speaking out, because I think that everyone in the Administration and in Congress needs to be speaking out.

COMMISSIONER TALENT: Sure.

MR CHU: But the coordination role, I think, does exist and needs to actually be the strengthened and expanded.

COMMISSIONER TALENT: Sure. I just had this idea sitting here. I mean, there would be a lot of things in the statute this person will be designated to do. And I'd be very interested to hear what Commissioner Wong thinks about it because of his experience. But please go ahead. And Mr. Davis, do you want to say something?

MR. DAVIS: Yes. I think it's actually a good idea. I wonder if it would be better if it were someone who dealt not just with Hong Kong, but perhaps China's periphery. So that there's sort of a coordinated effort. These things used to all be separated, but now I think they're coming together. And in the movement, the people that we work with, there, there are now a lot of interface between the various, the Xinjiang issue, the Uyghur issue, the issues in Hong Kong, and so on. So it's something we could think about, would be just how. Whether it should be, I mean, like my own work is on peripheral China. I look, I do Tibet as well. To look at how these communities are affected by Chinese policies. And then, a U.S., kind of, analysis and response.

MS. DATT: If I could just briefly add to that. I would think, you know, I think it's important to, you know, focus on the periphery. But also to acknowledge that a lot of the Chinese people are victims of the CCP's human rights violations. And that the -- you know, pro-democracy dissidents, the religious minorities, people within the proper mainland. It's also important to kind of maybe not combined with Hong Kong, but to also kind of speak out and put pressure for them.

COMMISSIONER TALENT: Okay, thank you.

VICE CHAIRMAN CLEVELAND: Commissioner Wessel? There you are.

COMMISSIONER WESSEL: I am here, thank you. Thank you to the Co Chairs for the hearing. To our staff, Alex, thank you for all you've done. And thank you to the witnesses. I have to say leave here very uneasy today from this panel. It sort of feels to me, and Mr. Chu, after your comments, a little bit of deja vu, if you will.

That we appear to be continuing to hold on to the hope that our continued treatment of Hong Kong in different ways will result in changes to the CCP's actions. It sort of reminds me of the old line that the CCP gets to have, eat their cake and have ours too. So we give Hong Kong a different customs tariff, we give them WTO membership. We treat them differently in terms of the 301 tariffs, as one of our witnesses talked about. None of us want to hurt the Hong Kong people. But are we rewarding the CCP for our failure to be more aggressive in terms of sanctions? They have. Shouldn't we be applying the 301 tariffs? Shouldn't we eliminate Hong Kong's WTO membership, which gives China, mainland China additional leverage and votes? Isn't a time that we understand, or you know, look at CCP's overall actions and view them as having a corrosive impact on the people? Mr. Davis, do you want to start?

MR. DAVIS: Well, I worry a little bit about how we banter the word sanctions about. I think sometimes that just gets us, kind of, in a tit for tat. That we post sanctions against

COMMISSIONER WESSEL: Then forget about, disregard the sanctions comment. And shouldn't we just treat Hong Kong as a part of the mainland as the CCP is doing?

MR. DAVIS: It's coming to that. I hate to see it. I lived in Hong Kong most of my life. And it's not mainland China. When I've traveled and worked in China, and I'd come back to Hong Kong, the difference is striking.

It's something, sometimes, it's hard to put your finger on it. But it's just very fundamentally it's an oasis, almost sigh of relief when people go back to Hong Kong from China because it's just such a remarkable place. So while I want to try to preserve that and put the pressure where needed to do so, I am also a little fearful of overshooting, and literally folding Hong Kong into the mainland. In some ways, some people say, well, Hong Kong would just become another mainland city. I fear that it'll be worse because other mainland cities don't have large groups of people that oppose the regime. So maybe Hong Kong becomes another Xinjiang or Tibet, rather than just another mainland city. So that would be tragic. I wish I could say how to convince the CCP to ease up on Hong Kong. But I do suspect we see some of it in the way they're dealing with Anti Sanctions Law. That some business methods may get their attention. And that's why I had earlier suggested, in my statement, I suggest maybe how we regulate business without using the language of sanctions.

But just what we expect of American businesses when it comes to protecting people's basic rights in how they conduct their corporate social responsibility, and so on.

So it's a complicated matter. But I think just pushing harder, just gets harder pushback. And I don't know how to get around that. I understand it. It's, I think, we're all perplexed by how to get around it.

COMMISSIONER WESSEL: Thank you. Mr. Chu?

MR. CHU: So I think I agree with Professor Davis on a point that I think is it's very important that we, for example, in the internet companies, I think that there still exists leverage points. Just a few months ago, the trade association for the tech companies made a statement or were quoted in the Wall Street Journal that Facebook and Twitter were thinking about retreating from Hong Kong.

Even though the individual companies themselves did not say that. But that provoked an immediate response from Hong Kong government. And said, oh, no, we're not doing any of the things that you're worried about.

And then, you know, the idea of, I think, those leverage points another example of that when the Joint Agency Business Advisory that came out a month and a half ago. All of those, I think, still provide a little bit of a view inside of how sensitive, at least some within the Hong Kong government, are still in terms of the perceptions and the trusted Hong Kong's status.

So I agree with Professor Davis. I mean, I don't have a magic bullet of how do you actually push back in overall, and restoring, and reversing all the trends that we're talking about here. But I also don't want to give up the leverage point that we still hold. And we continue to see, you know, that it matters to the Hong Kong government when the Heritage Foundation's dropped them from their economic freedom index.

And the talk about the kind of opinion pieces in Wall Street Journal that provoke a response from the Finance Minister in Hong Kong. And that, those pressure points continue to exist. And I think we have to deploy and use those tools as much as we can.

COMMISSIONER WESSEL: I hope you're right. Thank you.

VICE CHAIRMAN CLEVELAND: Thank you, Commissioner Wessel. Commissioner Wong?

COMMISSIONER WONG: Thank you. And thank you to our witnesses and your testimony. In listening to it, I am reminded of a quote, a famous one, from a former President of the United States. Where he said that freedom is not more than one generation away from extinction.

I'm reminded of that because with your focus on civil society, your rightful focus on civil society, speech, press, assembly, basic civil rights, those are the mechanisms by which Hong Kong will continue to transmit the unique spirit of Hong Kong.

In its embrace of liberty, that it's developed over three to four generations to the next generation, even if it is for now, under a more repressive hand.

So to that end, I wanted to ask a little bit more, and ask all of you to speak a little bit more, about what is the role of the churches in Hong Kong on this front?

And in particular, I'm thinking of the Christian churches, the Catholic Church, the Protestant denominations, the Anglican Church and others, to be loci of transmitting that spirit as it has in another context throughout history to transmit that spirit of liberty?

MR. CHU: So I will start, being I am the son of a Southern Baptist, of all things, Minister. I didn't learn until I came to the U.S. that we were called Southern Baptists not because Hong Kong is in the southern part of China. (Laughter.)

MR. CHU: And I, myself, went to seminary, continued that part of the family business before this part of the family business. I think that when my father first started in the pro democracy movement, 30 years ago, it was highly unusual for a Minister, for clergy to be publicly involved in political organizing. That has shifted slightly. It still has not become a mainstream, like you will see, for example, in the civil rights movement in the U.S. and other ways.

But I think that you are seeing a couple things that have happened. One is the regime had tried to incorporate the same tactic in the mainland that they're using where they were giving the religious church sector, a voice within the very narrow system that they had created to select a Chief Executive, for example. And by sort of buying their loyalty and allegiance, by giving them sort of a stated, state sponsored role, was one of the things that they tried to do.

And that, I think, still reflects sort of the mainstream of many of the denominations and churches on the ground. Which is that they stay out of politics. When they are given a role by the regime, they participate. The 2014, and then, the 2019 protest movement has opened up that slightly.

But we've also seen that that meant then the retaliation has come. The North Pointe District Church, which was one of the churches that were supporting protesters, shelters and financial support, their bank account was frozen at the end of last year. And the church actually announced that they were ceasing operation earlier this year. They were not the only church that have faced that.

And so I think we're at a point where because of the lack of previous, prior, sort of broad involvement of the churches, the regime, the government in Hong Kong has been able to really target and picked off any kind of what they consider liberal, progressive, radical voices.

The Hong Kong Pastors Network, as I mentioned, in my statement was a new network of pastors who have been vocal. They have now cease operations because they're afraid that even their online communication and posting would lead them to being arrested. And I think that that, you know, without even going into the whole debate and ongoing struggle between the Catholic Church and the Chinese regime, in terms of their appointments within the mainland and in Hong Kong, I think that that continues to be a challenge. And I think that people find it very difficult and risky to use the name and a banner of religion or church to be able to participate publicly.

MR. DAVIS: Well, as a Catholic, I guess I can comment on the Catholic Church's role. And I think Samuel already brought it up. They're wanting to participate and be on the mainland and have a connection with the mainland Catholic Church.

So I think, from Rome, there's been some pressure not to get too much into politics. But we know Cardinal Zen, famously, had been very much involved in the protest movement and been on the streets. I've met him on the streets. So he's --there is some element of activism within religion. But I think also important to understand that Hong Kong was not a very political place until, you know, very recent years. I can remember my first class in Hong Kong in 1985. I asked them if they would like to have the Sino British treaty or would they have something else? First, they rejected my question. They said, no one asked us. And then, finally, I said, well, humor me. And their vote was that they would return Hong Kong to China, and then, hire the British to run it. So you can see a kind of divided almost apolitical community. So the idea that religion sort of builds up to high engagement in politics takes time. It's not something that happens overnight. And now, with pressures to stay out of it, I would say their role will probably be diminished.

I know, the new head of the Catholic Church in Hong Kong is said to be more conservative and more cautious. So I'm not expecting a large role. But I think a lot of the parishioners I mean, it's oddly some of the leading figures. Martin Lee is a Catholic, very, a daily Catholic, goes to church every day. And the Chief Executive of Hong Kong is the Catholic. So religion, Hong Kong is like South Korea, one of the few Asian places where Christianity is very prominent, unlike on Mainland China, or Japan, and elsewhere. So there's potential there. But I think, somewhat diminished.

MS. DATT: If I could just briefly add, of the six websites that were blocked in Hong Kong, one of a Taiwanese church that had been raising funds to help protesters. I think, also regionally, it's something that the government is looking out for.

VICE CHAIRMAN CLEVELAND: Thank you. So turning to my questions, recognizing that time is short, I want to associate myself with what Commissioner Wessel identified.

His concerns about the fact that that we have Made in China labels coming through Hong Kong, but virtually nothing else has changed, whether its duties or WTO status, or any kind of economic leverage that might bring about or raise awareness in Beijing, so.

But I also understand that there's concern about the consequences of that for half of the tale of two cities. And it's less likely to impact the business community and more the quality of life for most Hong Kongers. So I wonder if there's a process both when it comes to freedom of speech and the internet, and when it comes to economic leverage that we could lay out a series of, if/then matrix. If we start to see the courts' views, subordinated to Beijing directive, then the following actions might be taken. Including, challenging or shifting WTO status.I think there's an update to Hong Kong Policy Act that is really what I'm hearing you articulate. And I think we need to try to pull it together.

The question, however, I have is, Mr. Chu, you mentioned that in the reference to collusion with foreigners, that that even contact with the United Nations can have consequences for the citizens of Hong Kong.

Senator Talent and Senator Goodwin had a very good hearing a couple of years ago on how China is trying to hollow out and change global standards and norms in international institutions. So I'm wondering if anybody is documenting the frequency which with contact with the American Consulate, the British Consulate, U.N. institutions is having consequences for Chinese citizens?

Is there any record that we could speak to? Because China, of course, stands up and says everybody welcomes our approach. I think there was an early, in very, very early days, our consulate was in touch with somebody who was immediately picked up.

So I'm wondering what kind of record there is of contact with international institutions or diplomatic consulates, offices of any kind, that that contact alone has consequences for Hong Kongers?

MR. CHU: I think that, so the easiest is obviously that we're seeing arrest warrants and charge papers in courts, specifically outlining contacts with, you know, outside groups or individuals.

So Jimmy Lai, who in one of his court appearances, the charge he actually has, is listed, a meeting with me in Washington, D.C. And so, I think that you see so that's one list that we are able to see.

The other I think is a little bit more subtle. I think it's intentionally vague, is the tactic here, that they would say, well, we're going to issue an arrest warrant for me. But then, what

about then the people that I come into contact with? My family members and people who are not even involved in the movement?

The U.S. Government, the administration, actually, and the State Department, have repeatedly, you know, assured me that they have tried to get clarification of what that means. But I think that they are trying to keep that intentionally broad and vague, so that we can't necessarily make all the connections and dots, you know, between the harassment arrests, the threats, and the contact.

So right now, I think that beyond the list of charges that are actually levered against the people who are in jail already or in courts, what we, I think, must do and do better of is, the tracking of threats to individuals, entities and persons.

And I think that that is something that we are starting to do. But it's not, I think, in a very systematic or robust way, I think, right now for Hong Kong.

MR. DAVIS: Yes, I would want to comment on that. The recent attacks on the Alliance in support of the patriotic democratic movement in China had tried to draw connection between them and the National Endowment for Democracy in the U.S.

And I had some personal experience with that, as well. In late 2019, I did a report that was jointly sponsored by the National Democratic Institute and Georgetown University.

When I was just having dinner in Hong Kong in the Mandarin Hotel, on my birthday, with Martin Lee, Margaret Ng, Lee Cheuk yan, and others who are old friends of mine, that made the entire front page of the Ta Kung Pao. Our pictures are spread all over it, so.

And we didn't even know. This Ta Kung Pao is newspaper, pro-communist, a communist owned newspaper. And we didn't even there was anyone there. Of course, it doesn't surprise us. But what I'm saying is they're monitoring very closely. That these

And this is in 2019, before the NSL. That people are just meeting, it was mostly a social meeting. But they're monitoring very closely any contacts with outside human rights organization. I think it bears important emphasis in any matrix, that people should not be punished for talking to international human rights NGOs, or organizations, or talking about human rights in Hong Kong, full stop. It should not be any kind of crime to talk to anyone about human rights. Chinese government is obligated under the Sino British Joint Declaration to uphold the ICCPR. And Hong Kong has reports under the ICCPR.

If the government can report on Hong Kong's human rights record, the people of Hong Kong should be allowed to report, as well. So I think if we want to any matrix that I think would be usable. And then, if people are arrested, or punished or sentenced, we should even be demanding their release. And if they can't be released in Hong Kong, they should be released over here. So allowed to go into exile and not held in jail.

Right now, almost the entire opposition movement in Hong Kong is locked up. And it's locked up for promoting human rights, full stop. It's, that's it. Jimmy Lai's heinous crimes, he's accused of being a dangerous man. His danger is simply reporting on human rights violations. So I think that contacts with -- and now, the Alliance case is directly, allegedly on point. And I think the Civil Human Rights Front, it's going to be the same. They're going to argue that they're receiving support or sponsorship.

Even when I was a fellow at the I was a Reagan-Fascell Fellow at one point, a couple years back. I was attacked for being involved with the National Endowment for Democracy. And I didn't control anything at the National Endowment. I had no involvement with them except to be a fellow. So this is a very sharply targeted area. And now it's showing up in all

these prosecutions where they're investigating organizations. And there's a whole list of organizations that are being investigated.

MS. DATT: And just to add, there is one resource in relation to the United Nations, which is they every year produce a report about reprisals, which are specifically attacks, or harassment of activists for trying to engage with the U.N. So any kind of incident of a Hong Konger trying to submit a report, or speak to a visiting official, or even to hold an event to talk about human rights, in theory, the U.N. should be documenting this and raising it to the Chinese government.

VICE CHAIRMAN CLEVELAND: If we all lived in the land of in theory. I very much appreciate all of your testimony. And it is powerful. And certainly with this audience, persuasive. We have a lot to think about in terms of recommendations. Ms. Thorson, not to forget you on the line there.

So I think we probably will follow up with some quick turnaround for the record since we are finishing up editing on our report. So I'd appreciate if you are able to respond with speed.

And we will take, well, a short break. I think, let's take five minutes. And then, Commissioner Glas, over to you to introduce the next panel. So we'll reconvene at -- I have three different times here. Well, how about -- that says 10:50. How about 10:55? Since all clocks are different here. Does that work? We'll take five minutes, and then reconvene. Thank you.

(Whereupon, the above-entitled matter went off the record at 10:53 a.m. and resumed at 10:59 a.m.)

PANEL II INTRODUCTION BY COMMISSIONER KIMBERLY T. GLAS

COMMISSIONER GLAS: Good morning. Our second panel will examine the importance the Chinese Communist Party ascribes to controlling sensitive data in economic markets. For our first witness, we recommend Dan Harris, partner at Harris Bricken.

Mr. Harris is internationally regarded as a leading authority on legal matters related to doing business in emerging markets. He writes and speaks extensively on international law with focus on protecting businesses in their foreign operations. And he has had the rare honor of being designated as a super lawyer. His China Law Blog co-authored by HB Lawyer Steven Dickinson is regarded as one of the best law blogs on the web today. Mr. Harris, thank you for speaking with us today.

Our second witness will be Rebecca Fair, CEO and co-founder of Thresher, a software company that combines unique datasets and machine learning to help decision makers in Government and Industry decode China even when others intentionally manipulate the narrative. She spent a decade as a CIA Officer in a variety of roles. She has also built, run, and then sold a management consulting practice for CEOs of mid-market companies. Ms. Fair, thank you for coming.

Finally, we will hear from Shaswat Das, counsel at King and Spalding. Shas has had a long career in U.S. Government and quasi-government agencies where he held numerous senior level positions, among other areas. He advises clients on compliance with U.S. economic and trade sanctions, anti-money laundering requirements, as well as federal securities and banking law regulations. Welcome back, Shas.

Again, please for our witnesses, keep your oral remarks to seven minutes. As some of you saw in the last session, we have a lot of questions and want to spend some time speaking to each of you.

Dan, before I turn it over to you, I want to acknowledge Vice Chairwoman Cleveland since you are going to be in the room, has graciously offered during the question and answer session to call on the various commissioners. So with that, Dan, thank you and we'll start with you.

OPENING STATEMENT OF DAN HARRIS, PARTNER, HARRIS BRICKEN

MR. HARRIS: Thank you, and thank you for having me. My name is Dan Harris. I'm an international lawyer and I have for the last 20 years been helping mostly American and European companies navigate China's legal landscape. I mention this up front because what I'm going to tell you today is based largely on what I've seen while representing companies who do or at least try to do business with or in China.

I will mostly be talking today about how China's Communist Party wields its laws and regulations to maximize its power and control to the detriment of foreign and domestic businesses. My firm's lawyers see the crushing of businesses in China every day and that has become increasingly true since President Xi became China's President in 2013. And especially since he effectively became President for life.

The CCP is cracking down on private businesses. We keep hearing about that and it is happening. By way of an example, my law firm has represented many of the big U.S. and Australian movie studios in their China legal matters and several of them have remarked to us how China hates foreign movie companies. After learning how difficult it is to make a movie that passes China's censorship requirements, our response has always been that China hates all movie companies because they can speak at least somewhat directly to the Chinese people.

China also does its utmost to wall off its internet from foreign companies. It does this by not giving foreign companies internet content provider licenses, which in turn forces them to pay Chinese companies that have their own ICP licenses. And they have to do that to legally get their web sites on internet servers within China. The CCP does this with ICP licenses to maintain control over online content.

Because Chinese domestic companies fear the CCP, they usually do not allow anything on the internet that the CCP might not want there. And if a Chinese company does put something on the internet that the CCP does not like, a Chinese government official can easily threaten that Chinese company with bad things if it doesn't stop or it can even arrest someone on the spot. Doing this is to accompany whose leadership in New York is considerably more complicated.

The Chinese company that allows a New York company to use its ICP license will make sure the New York company does not put anything on the internet that might offend the CCP. The CCP also does not allow foreign companies to operate schools that teach Chinese children. And it recently banned private tutoring in core school subjects.

Does China not care about foreign investment? We get asked that a lot. Does China not care about its own economy? The answer to these questions today is the same answer I would have given five, ten, and fifteen years ago. China cares about both foreign investment and its own economy, but only to the extent that those bolster CCP power and help ensure its survival.

As a lawyer, the best example I see of the tension between investment and economics on the one hand and CCP power and control on the other hand is actually China's court system. Our clients are always asking us about the fairness of China's courts and my answer has always been the same. If you are suing a Chinese company for breaching your contract to make rubber duckies, you will get a fair trial. If you are suing a Chinese company -- government company for stealing your cutting edge semiconductor IP, well good luck.

Many China lawyers call this the 90-10 rule. Ninety percent of the time, the Chinese courts will rule fairly because that allows its economy to function and that benefits the CCP. But

when the case is itself important for the CCP, fairness instantly gets tossed out the window. Legal scholars describe this as rule by law as opposed to rule of law.

The same is true for Chinese IPOs in the United States and for VIEs -- variable interest entities, I think they're called. China allows select companies to IPO in the U.S. often times via VIEs because it wants the money. But if for any reason the balance shifts to prohibiting either of these things, the CCP will do so.

VIEs are a classic example of how the CCP operates. China has allowed VIEs for at least a decade to secure foreign capital, but has never formally legalized them. And now that the CCP is making clear in various ways that it no longer values them as much, investors and underwriters are starting to panic. But this writing -- actually more accurately, the lack of any writing has been there all along for anyone interested in looking.

The same is generally true for China's new laws and regulations on data privacy, which are geared more towards giving the Chinese government access to data than towards protecting Chinese consumers. These recently revised regulations have not changed much, if at all, from those that preceded them.

The Chinese government has for years had essentially full access to all data, even data held by foreign companies operating overseas. The new laws mostly just reiterate and clarify this and shouldn't be viewed not so much as new laws, but as the CCP signaling that companies that collect data, the CCP does not want them to collect or that seek to hide data from the CCP are at increased risk of the Chinese government taking action against them.

What though should the U.S. government do about China? President Xi does not care about world opinion and he certainly does not care about being liked. He also does not care about following international law rules and customs. And why should he? When China's size and money and bullying have allowed them to get away with so much already. Because no country, including the United States, can exert much influence on Xi Jinping or the CCP, we should focus more on what we can do to keep growing our own economy, technology, and political standing. And less on how the U.S. can stop China from doing the same.

The U.S. government should encourage U.S. companies, even companies from other countries to cease doing business in or with China, especially manufacturing. The U.S. government should also be forthright with American people about how even if American companies reduce their manufacturing in China, we still should not expect a wholesale return of manufacturing to the United States. And every dollar that goes from China to Mexico or to Poland or to Thailand is a small victory for the United States.

Virtually all my clients who have their products manufactured in China would like to have them made somewhere else. And variably one of three things are stopping them from exiting China. One, the up-front cost of moving. Two, a lack of knowledge on where to go and how to find a good manufacturer elsewhere. And three, for many of them, there are no viable alternatives to China for manufacturing their products.

Number one above can -- number one can be ameliorated with subsidies and other incentives, the cost of moving out. Number two can be aided with information; how to figure out where to go. Number three will require the United States government to work with manufacturers in the United States and elsewhere to help them develop the necessary manufacturing capabilities.

One thing I would like to add to the prior discussion when talking about the Chinese government monitoring human rights activists, the Chinese government also monitors American companies even in the United States. If you talk to American companies, many of them will not

send their people to government offices in D.C. or at least they're reluctant to do so. And they often times like to send proxies because they're convinced that the Chinese government films who goes in and out. And they do not want to be seen as essentially fighting against China.

PREPARED STATEMENT OF DAN HARRIS, PARTNER, HARRIS BRICKEN

My name is Dan Harris. I am an international lawyer who has for the last 20 years been helping mostly American and European companies navigate China's legal landscape. I mention this upfront because what I am going to tell you today is based largely on what I have seen while representing companies that do -- or at least try to do -- business with or in China.

I will mostly be talking today about how China's Communist Party wields its laws and regulations to maximize its power and control to the detriment of foreign and domestic businesses. My firm's lawyers see the crushing of businesses in China every day and that has become increasingly true since Xi Jinping became China's president in 2013, and especially since he effectively became president for life in 2018.

1. The CCP is Cracking Down on Private Businesses

CCP antipathy towards private business is nothing new; it is as old as communism itself.

By way of an example, my law firm has represented most of the big US and Australian movie studios in their China legal matters and several of them have remarked how China "hates foreign movie companies" after learning how difficult it is to make a movie that passes Chinese censorship requirements. Our response has been that China hates all movie companies because they can speak somewhat directly to the Chinese people.

China also does its utmost to wall off its Internet from foreign companies. It does this by not giving foreign companies internet content provider (ICP) licenses, which in turn forces them to pay Chinese companies with their own ICP licenses to legally get their websites on Internet servers within China. The CCP does this with ICP licenses to maintain control online content. Because Chinese domestic companies fear the CCP they usually do not put anything on the Internet that the CCP does not want there. And if a Chinese company does put something on the Internet that the CCP does not like, a Chinese government official can threaten that Chinese company with bad things if it doesn't stop or even arrest someone on the spot. Doing this is a company whose leadership is in New York is considerably more complicated. The Chinese company that allows a New York company to use its ICP license will make sure the New York company does not put anything on the Internet that might offend the CCP.

The CCP also does not allow foreign companies to operate schools that teach Chinese children and it recently banned private tutoring in core school subjects.

Does China not care about foreign investment? Does China not care about its own economy? The answer to these questions today is the same answer I would have given 5, 10, and 15 years ago. China cares about both foreign investment and its own economy, but only to the extent that those bolster CCP power and help ensure its survival.

As a lawyer, the best example I see of the tension between investment and economics on the one hand and CCP power and control on the other hand is China's court system. Our clients are always asking us about the fairness of China's courts and my answer has always been the same. If you are suing a Chinese company for breaching your contract to make rubber duckies, you will get a fair trial. If you are suing a Chinese government company for stealing your cutting-edge semiconductor IP, well, good luck. Many China lawyers call this the 90-10 rule. Ninety percent of the time the Chinese courts will rule fairly because that allows its economy to function and that benefits the CCP. But when the case is itself important for the CCP, fairness instantly gets tossed out the window. Legal scholars describe this as rule by law, as opposed to rule of law.

The same is true for Chinese IPOs in the United States and for VIEs. China allows select companies to IPO in the US -- oftentimes via VIEs – because it wants the money. But if for any reason the balance shifts to prohibiting either of these things, the CCP will do so.

VIEs are a classic example of how the CCP operates. China has allowed VIEs for at least a decade to secure foreign capital. But it has never formally legalized them and now that the CCP is making clear in various ways it no longer values them as much, investors and underwriters are panicking. But this writing – actually, more accurately the lack of any writing – has been there all along for anyone interested in looking.

The same is generally true for China's new laws and regulations on data privacy, which are geared more towards giving the Chinese government access to data than towards protecting Chinese consumers. These recently revised regulations have not changed much, if at all from those that preceded them. The Chinese government has for years had essentially full access to all data, even data held buy foreign companies operating overseas. The new laws mostly just reiterate and clarify this and should be viewed not so much as new laws, but as the CCP signaling that companies that collect data the CCP does not want them to collect or that seek to hide data from the CCP are at increased risk of the Chinese government taking action against them.

2. **Why is the CCP Accelerating its Crackdown on Private Businesses?**

First off, let me make clear again that the CCP has been cracking down on private businesses and free speech and the rule of law pretty much since Xi Jinping assumed power.

The CCP's recent crackdowns on private businesses should not be at all surprising both because similar crackdowns have been going on for so long and because they were entirely predictable. What I find *more* surprising is how so many people are expressing surprise about the crackdowns. When people tell me they did not see this coming, my response is "right, I mean how could you possibly have known there were communists in China?" "And why should you not expect a country that is – at the very minimum –

engaging in a cultural genocide against its Uyghur and Tibetan populations to respect private property, private businesses, and the rule of law?"
On July 27, in a piece entitled *Wall Street Gets a Chinese Education: The Communist Party Control Always Trumps the Needs of Investors*, the Wall Street Journal's Editorial Board had this to say about the CCP's antipathy towards private business and lack of concern for the economy: "The big surprise from this week's slump in Chinese company stocks is that people are claiming to be surprised. President Xi Jinping has made plain for years that he intends to bring ever greater swathes of China's private economy under the state's control. Guess what, Wall Street: He meant it."

Western businesspeople have been getting China wrong for a long time, largely because they tend to assume everyone acts out of economic self-interest. But for the CCP, the economy is a means to an end, with the end being a socialist state fully controlled by the CCP. Do not forget: Xi Jinping and the CCP are Marxists and Marxists believe that after capitalism comes socialism and after that stateless communism. China has been moving along Marx's stages of development since Mao, and Xi Jinping appears to believe China is nearing the socialism stage, so it can start tossing out more and more capitalist elements and that is exactly what its crackdown on private businesses is doing. The West's recent efforts to disengage from China are another reason why the CCP is accelerating this crackdown now.

Did foreign investors not know these things about China? Many did not. Businesspeople and investors typically are trained to look at industries and companies, not governments.

However, many did know, but for monetary reasons, did not want others to know. I say this because when my firm's lawyers write anything remotely critical of China, expats in China often will tell us they wish we hadn't because our articles might encourage their companies to pull out of China and they may be out of a job. Few businesspeople have any incentive to tell the truth about China.

3. What Should the U.S. Government do About China?

Xi Jinping does not care about world opinion, and he certainly does not care about being liked. He also does not care about following international law, rules, or customs. And why should he, when China's size and money and bullying have allowed them to get away with so much already? Because no country, including the United States, can exert much influence on Xi Jinping or the CCP, we should focus more on what we can do to keep growing our own economy, technology and political standing and less on how the U.S. can stop China from doing the same.

The U.S. government should encourage U.S. companies -- and even companies from other countries – to cease doing business in or with China, especially manufacturing. The U.S. government should be forthright with the American people about how -- even if American companies reduce their manufacturing in China -- we still should not expect a

wholesale return of manufacturing to the United States. But every dollar that goes from China to Mexico or Poland or Thailand is a victory for the United States.

Virtually all my clients who have their products manufactured in China would like to have them made somewhere else. Invariably, one of three things are stopping them from exiting China. One, the upfront costs of moving. Two, a lack of knowledge on where to go and how to find a good manufacturer elsewhere. And three, there are currently no viable alternatives to China for manufacturing their products.

Number one above can be ameliorated with subsidies and other incentives. Number two can be aided with information. Number three will require the United States government to work with manufacturers in the United States and elsewhere to help them develop the necessary manufacturing capabilities.

The U.S. Government also should do more to protect U.S. investors from publicly traded Chinese companies. It makes no sense for Chinese companies on U.S. exchanges to have lesser auditing requirements than other companies, but they do, and few know this. As someone who has literally never seen a Chinese company accounting records that are not at least highly suspect, I think Chinese companies should be removed from all U.S. stock exchanges. But if they are to be allowed, they should at least be required to meet the same standards as other companies and the SEC should alert investors to their special risks.

The U.S. Government also must do more to protect its own citizens and companies from China. It did so by blocking a Chinese company from purchasing Tinder, but this is just the tip of the iceberg in terms of how China uses its "private" companies to digitally invade the United States. Chinese companies are scooping up personal information about Americans with little being done to stop them. For example, and as was pointed out by Voice of America, "A Chinese gene company is collecting genetic data through prenatal tests from women in more than 50 countries for research on the traits of populations, raising concern that such a large DNA database could give China a technological advantage and the strategic edge to dominate global pharmaceuticals, according to a recent news report." Tik Tok is also a threat, as are other Chinese companies that operate in the United States, ostensibly for profit, but more likely to gather intelligence. We have to recognize that Chinese private companies – even the many that wish it were otherwise – are in no position to say "no" to the CCP.

OPENING STATEMENT OF REBECCA FAIR, CEO AND COFOUNDER, THRESHER

COMMISSIONER GLAS: Thank you so much, Mr. Harris. Ms. Fair?

MS. FAIR: Thank you. Thank you, Vice Chairman Cleveland and Commissioner Glas. It's an honor to join you this morning to participate in this esteemed panel, alongside Dan and Shas. My aim today is to shed light on the ways the Chinese government is manipulating the landscape in which businesses are operating in China and here in the U.S.

I'm approaching this subject from my vantage at Thresher, a company that monitors how the Chinese government manipulates social media conversations, especially in China. Understanding what Beijing is censoring and amplifying at home can offer important insights into its goals and vulnerabilities globally.

We all know that China seeks to control its economy. One of the key levers of that control is information about the players in its economy. China is spending billions of dollars each year -- that's billions with a "B" -- to control its information environment. It deploys artificial intelligence and tens of thousands of people to generate, moderate, and sensor staggering amounts of information every day.

Content moderation is not unique to Chinese media platforms. All media platforms moderate content to keep illegal content out. But Chinese media platforms must also moderate content based on the direction from the Chinese government. The content of the Chinese government is manipulating touches on a range of concerns from military exercises to education initiatives, from celebrity culture to COVID-19. But there are particularly important insights that we can draw from their manipulation of the business landscape.

I invite you to consider the recent example of Didi, a Chinese ride-sharing app like Lyft or Uber that listed on the New York Stock Exchange in defiance of the Chinese government. In response, Beijing opened a national security investigation into Didi. Then it flooded social media with propaganda about that investigation and allowed the spread of disinformation about Didi.

That disinformation claimed that in order to list on the New York Stock Exchange, Didi agreed to give the U.S. government access to its users' data. Didi leadership tried to publicly deny that disinformation, but the Chinese censored online content talking about Didi's denial.

In this example, we see the trifecta of the Chinese government's manipulation toolkit; propaganda, disinformation, and censorship. Propaganda that amplifies its narrative and drowns out other voices. Disinformation that fires up the Chinese people against Beijing's target. And censorship that removes any competing narratives. Sometimes together, sometimes independently, these techniques enable the government to control the players in its economy, a key element of its strategy to control the economy as a whole.

Furthermore, our data shows that these techniques are effective with the Chinese public. Our AI reviewed millions of Chinese social media posts in July and detected no discussions that expressed concern about the Chinese government's targeting of Didi or its ability to access user data. However, it did find discussions where users were worried about U.S. government access to Chinese data.

Simply put, the Chinese government is using its manipulation toolkit to shape the Chinese public's views on Chinese companies, the tech sector, the U.S. government, and data privacy standards. Beijing is also using this toolkit sometimes for and sometimes against U.S. companies. The toolkit is another carrot and stick or stick that Beijing can use to control U.S. companies.

Earlier this year, there was a spike in online conversation about companies that use cotton-produced in Xinjiang region where the Chinese government is using the Uyghur people as forced labor. Chinese social media users expressed outrage, not at the use of forced labor, but at foreign companies, including U.S. companies like Nike who announced that they would stop sourcing cotton from the region. Chinese netizens called for boycotts of Nike and other brands. And the Chinese government did not censor these calls or otherwise reshape the conversation.

However, Beijing has censored calls on social media for boycotts of other American brands, including for example Disney. In 2019, Disneyland Hong Kong allowed its workers to attend protests against a proposed bill that would have allowed extradition of people from Hong Kong to mainland China.

Some Chinese social media users argued that by allowing its workers to protest the bill, Disney implicitly endorsed Hong Kong's independence. These same users then called for boycotts of Disney. Beijing stepped in and censored these calls, partly to tamp down the controversy about extradition and party to protect the reputation of the U.S. company.

We already know that a good relationship with the Chinese government is key to doing business in China. Now American companies doing business in China must navigate a political environment where Beijing can mobilize public support for or against a brand with a few key strokes.

American companies also face intense pressure to make their data, including user data accessible to the Chinese government. After considering how China seeks to control companies doing business in the U.S. and control U.S. companies doing business in China, the implications and risks to U.S. interests come into focus.

For American consumers and investors who would like to do business with Chinese companies here in the U.S., China's information manipulation poses different threats. There are valid concerns about the Chinese government's ability to collect and exploit data from Chinese companies, including data collected from customers in the U.S.

It can also be difficult for Americans who invest in or partner with Chinese companies to attain the degree of accountability they expect of their partnerships, especially when the information environment back home is so susceptible to manipulation. I'm sure my fellow panelists will have more to add on these -- precise nature of these and others risks.

So what's to be done? With the Chinese government's demonstrated ability to meddle in markets, control companies, and shape the narrative around its efforts, we here in the U.S. and the U.S. government in particular must have the best and most complete data about the information environment, so that we can accurately assess what is being manipulated and why.

That's why I recommend creating a clearing house for collecting, sharing, and analyzing data about the Chinese economy and Chinese companies that operate in the U.S. and other markets outside of China. A centralized approach to this kind of data can help us understand China's goals and monitor their evolving tactics. Understanding based on data, not anecdotal reporting is key to formulating our own response, protecting our financial systems, and combating Beijing's efforts to manipulate global markets.

Second, I recommend establishing clear standards for data collection and protection here in the U.S. Establishing our own standards is a necessary first step towards shaping data and privacy standards worldwide. Shaping worldwide standards is very much in our national interest and it's something that China is already trying to do in line with its values, not ours.

There is of course much more to say about China's manipulation of the information environment and its impact on the U.S. economy, U.S. companies, and U.S. citizens, but I'll pause here. Thank you very much. I look forward to your questions.

PREPARED STATEMENT OF REBECCA FAIR, CEO AND COFOUNDER, THRESHER

Media Manipulation Monitor

Rebecca Fair, CEO and Cofounder, Thresher

Testimony before the U.S.-China Economic and Security Review Commission

Hearing on U.S.-China Relations in 2021: Emerging Risks

August 24, 2021

What you need to know: China seeks to control the players in its economy. As part of this effort, the Chinese government is increasingly trying to control Chinese companies' involvement in the US market and to retaliate against US companies in China's markets—such as with China's forthcoming anti-sanctions law.[1] A key component of controlling the players is controlling information about the players. China spends billions annually to control its information environment, deploying AI and humans to generate and moderate huge volumes of content. Beijing uses this information control machine to attempt to shape the conversation about the Chinese economy as well as Chinese, US, and other companies in the China and US markets. Distorting economic and financial information makes it difficult for the US government and US companies to make good decisions, because good decision making relies on good data.

What the data shows: The Chinese government has pushed the narrative in Chinese media and social platforms that tech companies listed on the NYSE are national security liabilities for China because the US government and US-based investors can demand access to the Chinese companies' data. The Chinese government seeks to crack down on companies and tech leaders, such as Jack Ma, Ant Financial, Alibaba, Didi, and others, who do not fully comply with Beijing's rules and data regulations. Chinese netizens express more support for than opposition to the government's crackdown and have derided US-based tech companies who threatened to pull out of the Hong Kong market. At the same time, the Chinese government has prevented potential dissenting views from forming by censoring news on Chinese social media that suggested these industry leaders' innocence.

What we recommend: With such sweeping and sophisticated efforts from China to meddle in markets, control companies, and shape the narrative around its efforts, it is vital to support, combine, and share the data collected across the US government to monitor, evaluate, and disrupt China's information control efforts. Therefore, we recommend that Congress consider:

- **Creating a clearing house aimed at collecting, sharing, and analyzing data about Chinese companies as they operate in US and other non-Chinese markets.** Data will help our government build a clear view of the playing field that they can use to inform timely policies to protect our financial systems and companies and to combat Beijing's

[1] "Do not mistake delay to anti-sanctions law for Hong Kong as climbdown by China, analysts say, as targeted weapons against Western powers still in works," South China Morning Post, https://www.scmp.com/news/hong-kong/politics/article/3145849/do-not-mistake-delay-anti-sanctions-law-hong-kong-climbdown

efforts to meddle in markets and control the related narrative. This clearing house could work as a central point to understand the evolving threat landscape affecting national financial institutions, strategically important economic sectors and industries, and the American economy as a whole. There may be a partnership opportunity with the National Economic Security and Financial Intelligence Executive.

- **Establishing standards for data collection and protection. Establishing our own standard will help the US lead the ongoing evolution of tech companies' data and privacy standards worldwide—an evolution that China is currently trying to control.** For example, Hong Kong recently passed a new data privacy law that was rejected by US tech companies, including Google, Twitter, and Facebook.

Background on Thresher's Media Manipulation Monitor (M3) Insights and Data: Thresher's M3 tracks Chinese government manipulation—such as censorship, propaganda, and inauthentic amplification—of traditional and social media, as well as other types of data. Our system provides a unique look at the PRC's objectives, sensitivities, and vulnerabilities, which we uncover as we monitor what information it seeks to control, silence, and spread online—at home and abroad.

Didi Chuxing: A case study on how the PRC uses information manipulation to advance its economic goals

The Chinese government is interested in the power and wealth of US capital markets, but wary about the political leverage it gives Chinese companies. Under General Secretary Xi Jinping, the state has increasingly regulated China's private sector to diminish what Xi calls the "disorderly expansion of capital"[2] and decrease foreign influence on China. This regulatory trend gained international attention in July 2021 when Beijing punished one of its tech champions, ride-sharing company Didi Chuxing, for listing on the New York Stock Exchange without the appropriate government offices' approval.

The example of Didi Chuxing offers a case study in how the PRC uses manipulation of social media to advance its economic goals—in this case, attacking a previously lionized domestic tech company for engaging in the US economy in a manner that extends beyond Beijing's control. Our analysis of 250 million Chinese social media posts found the following insights based on the PRC's manipulation patterns during Beijing's July 2021 crackdown on Didi Chuxing's IPO:

Insight 1: The Chinese government manipulates social media to try to turn the public against Didi and further its narrative about the need for Beijing to centralize control of tech data policy. *Page 5*

[2] "China to strengthen anti-monopoly push, prevent disorderly capital expansion," Xinhua, http://www.xinhuanet.com/english/2021-03/05/c_139784906.htm

---

Insight 2: Chinese netizens largely support their government's crackdown on Didi and its increased regulation of the tech sector. *Page 5*

- Chinese netizens' online behavior indicates they support Beijing's increased regulation of the tech sector to protect data privacy. *Page 6*
- Chinese netizens showed greater engagement with government-authored content about app data protection and regulation in 2021 than in years prior on similar content. *Page 7*

Insight 3: The PRC seeks to downplay the narrative that its regulatory actions introduce new or heightened risk to China markets by censoring alternate narratives and amplifying its propaganda. *Page 7*

Insight 4: The Chinese government is censoring case details and rumors, attempting to forestall public calls for additional investigations into Didi that may reveal additional concerns or further infractions. *Page 8*

Timeline of Beijing's manipulation of the Didi narrative

29 June 2021: Censors removed netizen discussion that Didi gifted many executives large numbers of shares during its IPO. Very heavy censorship: 51% / 694 interactions

2–3 July: Government-affiliated accounts on Chinese social media amplified news that the Central Cyberspace Affairs Commission (CAC) announced an investigation of Didi, purportedly for national security reasons. Elevated amplification: 172 posts / 176,000 interactions

2–9 July: Chinese netizens reacted to news of the Didi crackdown with mostly supportive or neutral sentiment. No significant dissent detected. 14,000 netizen posts / 6 million interactions

3–4 July: Censors quashed discussion of Didi's Vice President Li Min denying that Didi granted the US government access to Didi users' data. Very heavy censorship: 50% / 156,000 interactions

4–6 July: Government accounts amplified news of the investigation again, adding that Didi should be removed from app stores in China. Extensive amplification: 1,055 posts / 2 million interactions

5 July: Censors removed netizen discussion about Didi's research lab in California. Heavy censorship: 13% / 8,900 interactions

5–7 July: Chinese netizens expressed derision toward Facebook, Google, and Twitter for threatening to pull out of the Hong Kong market in light of Hong Kong's new Data Privacy Law.[3] 186 netizen posts / 45,000 interactions

17–19 July: Government accounts amplified a warning to consumers about how tech companies can trick app users into giving over personal information. Heavy amplification: 358 posts / 93,000 interactions

24–25 July: Censors removed netizens' discussion on Chinese social media that Merrill Lynch and JP Morgan purportedly warned their investors against entering China markets. Very heavy censorship: 47% / 6,000 interactions

[3] "Facebook, Twitter, Google Threaten to Quit Hong Kong Over Proposed Data Laws," The Wall Street Journal, https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036

Insight 1: The Chinese government manipulated social media to try to turn the public against Didi and further its data centralization narrative.

The Chinese government amplified the narrative that Didi illegally collected users' personal data while censoring Didi's announcement that it would never hand users' data over to the US government.

- **Amplified:** Chinese government-affiliated social media accounts on 2 July 2021 announced and amplified the narrative that Didi had committed various crimes, in particular regarding users' data privacy. The headlines about Didi Chinese state media amplified most heavily in July 2021 were:

Highest post volume campaigns	Chinese
Cyberspace Administration of China: Remove the Didi app from App stores	国家网信办：#滴滴出行App下架#
CCTV exposes: Cell phone apps that carry three traps. Have you fallen into these traps?	#央视曝App弹窗广告三大陷阱# 你中过招吗？
Seven government departments jointly station in Didi's offices to carry out investigation	#七部门联合进驻滴滴开展网络安全审查#
Remove Didi and these 25 other apps from your stores	#下架滴滴顺风车等25款App#
Cyberspace Administration of China: Take Didi off the [app store] shelves!	国家网信办：滴滴出行，下架！

Insight 2: Chinese netizens largely support their government's crackdown on Didi and increased regulation of the tech sector.

Chinese netizens expressed support for the government's narrative that Didi provided, or might provide, user data to the US government in order to list on the New York Stock Exchange. Chinese netizens support the government's crackdown on Didi as a measure that protects China from US influence.

- **Netizens expressed support.** A random sample from 6,000 netizen posts showed 56% expressing neutral sentiment toward the Didi crackdown and 44% expressing support. Nearly no posts expressed dissent.

- **We assess that the lack of detected dissent was not due to censorship.** M3 algorithms and data collection methods reveal PRC efforts to remove content that expresses disapproval of government action; in this case, M3 did not detect censorship of dissenting opinions.

- **However, censors removed news that might have fueled dissent.** On 3 July, China's internet authorities censored news that Didi's Vice President Li Min said Didi would never hand users' data over to the US government, aiming to limit content that undermined Beijing's claims that Didi had violated data privacy standards.

    - Netizens expressed mixed opinions about the credibility of Li's statement, with some saying it was impossible to give the US access to data stored in China and others saying that Li was lying to defend himself.

    - This news was widely discussed and heavily censored, making it among the top 5% of most manipulated discussions on Chinese social media in 2021.

Chinese netizens support the increased regulation of the tech sector to protect data privacy. There is little debate on Chinese social media about the pros and cons of increased government regulation of the tech sector because Chinese netizens are accustomed to the concept of government control but are wary of private sector overreach.

- M3 detected no netizen discussions in July 2021 that expressed concern about Chinese government access to private data, but netizens did express concern about potential US government access to Chinese data. (Any censored conversations would have been captured by M3.)

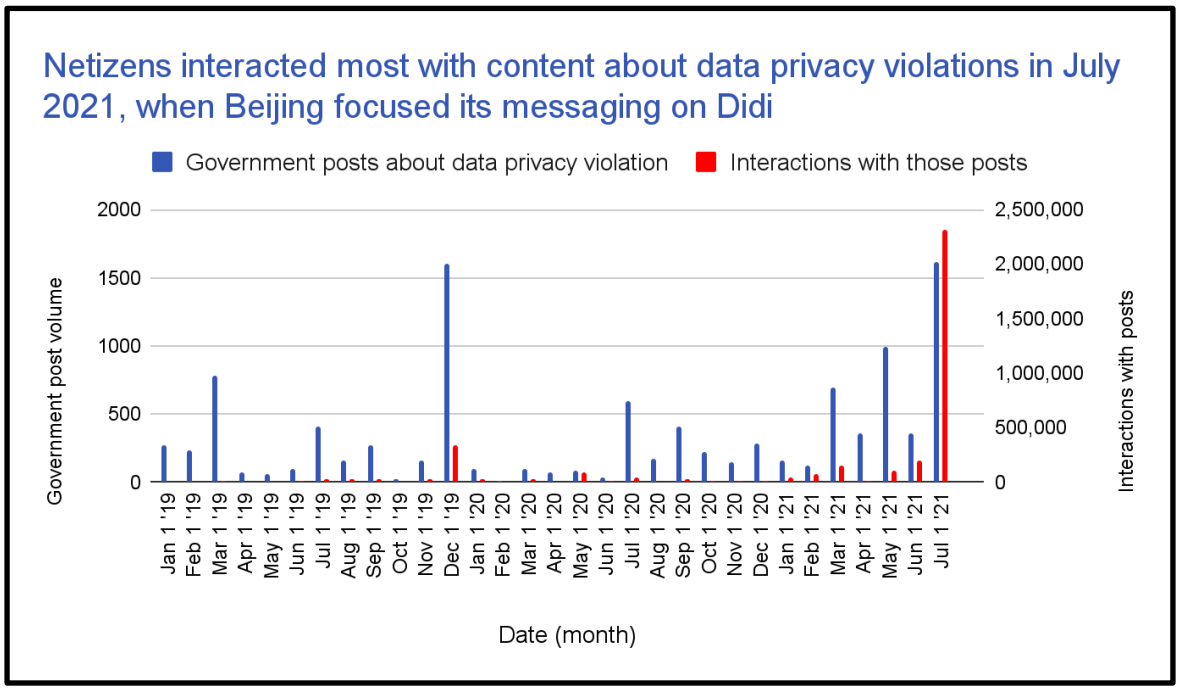
- Netizens expressed derision toward Facebook, Google, and Twitter on 5–7 July 2021 for opposing the Hong Kong data privacy law. Many expressed hope that these three US companies would pull out of Hong Kong, opening the market for Chinese competitors and depriving democracy advocates—who many mainland Chinese netizens see as separatists—of an online forum.

Chinese netizens showed greater engagement with government-authored content about app data protection and regulation in 2021 than in years prior on similar content.

Beijing has launched several crackdowns on hundreds of apps that violate users' privacy in the past few years, typically on apps that are not market leaders. Chinese government accounts have authored 10,800 posts about apps violating users' data privacy since 1 January 2019. Netizen engagement peaked when Beijing targeted Didi.

- In December 2019, Beijing launched a campaign against apps that violated users' data privacy, removing 100 apps from the market and educating the public about how to spot violations.

- In July 2020, Beijing launched another campaign, removing 260 apps from the market for user data privacy violations.
- Beijing ramped up its warnings and admonishments of user privacy violations in 2021 Q1 and Q2, but netizen engagement increased twenty-fold when Didi became the target.



Insight 3: The PRC seeks to downplay the narrative that its regulatory actions introduce new or heightened risk to China markets.

While most Chinese netizens agree with the crackdown on Didi and do not oppose government-led data regulation, debate exists on Chinese social media regarding the speed of Chinese government regulations and its economic repercussions.

- On 24–25 July 2021, China's censors quashed netizen discussion about the US investment management companies Merrill Lynch and JP Morgan, which purportedly issued warnings about China investment risk due to the Chinese government's unpredictability. Censors removed the narrative that Beijing's actions introduce new or heightened risk to China markets.

Insight 4: The Chinese government is censoring Didi case details and rumors to cut off public demand for more investigations into the company.

China's internet authorities censored rumors about Didi's specific wrongdoings beyond "the serious violation of the illegal collection of personal information"[4]—as Beijing currently describes

[4] "严重违法违规收集使用个人信息问题"

the crime—to prevent the public from demanding the government investigate specific aspects of the Didi case. Open discussion of specific case details and rumors, such as Didi giving away shares and its research lab in the US, likely would make the government's messaging around the Didi case more difficult—for example, if it turns out that government officials were involved.

Context: The Chinese government frequently obfuscates details of legal cases to prevent public inquiry that might result in citizens demanding the government take certain actions, whether stronger or softer on the defendant.

Data:

- Censors on 29 June—the day before Didi's IPO—removed netizen discussion that said Didi had gifted many of its executives large shares of the company. Censors removed this discussion to quell netizen anger about unequal distribution of wealth and corporate cronyism, in particular regarding large tech companies. **Very heavy censorship: 51%**
- Censors on 5 July—a few days after the government kicked off its crackdown on Didi—removed netizen discussion about Didi's research lab in California. Some netizens surmised that the lab had access to Chinese government officials' private data and that the lab's location in California meant the US also had access to that data. Censors removed these posts probably to avoid netizen demands that Beijing force Didi to close down the California lab, either because China seeks to maintain access to US talent and technology or because it is developing a plan to bring overseas companies home but not ready to act.[5] **Heavy censorship: 12%**

[5] "What is China's 'battle for data' and who will be targeted next?," California News Times, https://californianewstimes.com/what-is-chinas-battle-for-data-and-who-will-be-targeted-next/461195/

OPENING STATEMENT OF SHASWAT DAS, COUNSEL, KING & SPALDING

COMMISSIONER GLAS: Thank you so much, Ms. Fair. And I'm going to recognize Shaswat. Thank you so much for coming back to the Commission. And I appreciate Mr. Harris and Ms. Fair's testimony.

MR. DAS: I should note at the outset that the views expressed here are solely my own and do not necessarily reflect the views of my colleagues or law firm.

Today I will touch on three major topics; China's regulatory -- changing regulatory approach towards Chinese listings in the U.S., the future of the VIE structure, and the delisting process and the consequences. But first, I'd like to start with a 30,000 foot view of U.S. China relations, which bears heavily on each of these topics.

To that end, I will discuss why China's acting the way it is. And sometimes in a manner that seems contrary to its own economic interests. China with a rich and varied history does not fit so easily into the capitalist mode as is apparent. It is through this lens that we are able to more clearly understand China's actions; the ones they've already taken and the ones that they will take in the future.

In mid-August for example, President Xi commented that Beijing will increasingly promote social equality using the new catch phrase, "common prosperity" in an attempt to portray China as a socialist country. Despite this statement, China most definitely remains a communist country where property and economic resources are either owned or controlled by the state.

To skip ahead a bit, it is my belief that China has for the past several years viewed U.S. capital markets as a relatively easy source of funds. In light of increased scrutiny of Chinese companies listed on U.S. exchanges, the most likely course of events is for China to retrench, forcing their companies to list on Shenzhen's ChiNext, Shanghai's STAR market in Hong Kong or other non-U.S. exchanges.

Said differently, while China certainly cares about economic power, it also cares about issues such as pride, security, and most importantly, control. They appear willing to sacrifice the monetary gains that accrue from U.S. listings if doing so will in their view, better protect other values consistent with its authoritarian society. Thus any future negotiations regarding U.S. inspections of the Chinese companies audits are likely to be unsuccessful without major compromises on both sides.

With regards to its evolving regulatory approach, China is quite clearly taking a more aggressive regulatory stance of late with one agency in particular playing a very prominent role. As was just noted, the most recent examples are the actions taken against the ride-hailing company, Didi with the Chinese government announcing an investigation into the company's data security practices and then mandating that the app be removed just days after the company raised $4.4 billion in its U.S. IPO.

This has been followed by a new regulation that requires all companies with data on more than 1 million users, so effectively all Chinese internet companies, to seek formal approval from the Cyberspace Administration of China, the CAC, before pursuing a foreign listing.

The CAC's been around since 2011, but only recently has come to wield such outside influence. Other regulations include the State Administration of Market Regulation, basically the anti-trust unit, as well as the financial and trade regulators such as the China Securities Regulatory Commission, Ministry of Finance, and Ministry of Commerce.

It is not so important who the regulators are as to what matters to them. In the recent elevation of the CAC sends a clear message that for China, data security trumps financial gains or at least that is the message that they want to send. The reality however may be quite different. I generally believe that this is all political or pretextual rather than a genuine concern over data protection.

With the prospect of delistings now on the horizon, the Chinese Communist Party is accepting of its scrutiny of Chinese companies listed in the U.S. largely in response to the actions of the U.S. government, including but not limited to, the moratorium on the new IPOs until such companies beef up their risk disclosures and separately the issuance of the Chinese military industrial complex list. The CCP wants to control the narrative and be able to argue that they brought these companies back home on its own terms, rather than because they were threatened with delisting by U.S. regulators.

Now with regard to the future of the VIE structure, the VIE is the primary method that Chinese companies use to get around rules that forbid foreign ownership of Chinese companies. It's been in operation and use for now close to 20 years. The VIEs are 100 percent owned by Chinese individual or in some cases such as Alibaba, entities owned by Chinese individuals, usually but, not always, the founder and chairman.

The shares sold to U.S. investors are part of a wholly-owned foreign-owned enterprise, often referred to as WFOE, which is the Chinese subsidiary of the offshore shell company that is generally incorporated in the Cayman Islands. In most cases, the VIE owns effectively all of the business through a set of contractual agreements with the wholly foreign-owned enterprise acting as a sort of tracking stalk that fluctuates, along with the underlying companies business, which has no claim on any significant business assets.

Presently, VIE arrangements transfer control to the wholly foreign-owned enterprise and indirectly to the offshore parent, which remains in the hands of Chinese nationals. The equity ownership of these companies is held by China-based shareholders.

While the VIE shell companies do have contractual rights, the enforcement of these rights is hardly questionable. Indeed many perspectives of these companies are replete with warnings about the lack of shareholder rights.

Picking almost at random from the perspectives of electrical vehicle maker, NIO, shareholders are warned that they have no general rights under Cayman Island laws to inspect corporate records or obtain copies of list of shareholders, or that it may be difficult or impossible for U.S. investors to bring an action against them in the United States or it would be difficult for U.S. shareholders to initiate actions against the PRC in accordance with PRC laws.

It is also worth noting that Chinese regulators have never objected to the VIE structure to any effect. Also they've never blessed it. It is therefore possible, however unlikely it may seem, that they could one day simply invalidate VIEs leaving U.S. investors holding an empty bag.

This scenario is difficult to imagine given that such a step would affect all foreign investors, not just those located in the U.S., effectively cutting off Chinese company access to global financial markets. Rather, it is far more likely that the Chinese government will tighten the rules for its companies listed overseas.

Now onto the delisting process and companies that may go private or in conversions of ADRs of Chinese companies listed in the U.S. The future of the VIE structure really leads directly to the question of how companies are removed from U.S. exchanges. As mentioned, while the VIE has been a useful construct for Chinese companies over the past two decades. Much of the value from China's point of view has been the ability to evade measures such as

U.S. audits of Chinese firms. Now that this is being threatened, the VIE structure holds far less appeal for China in the current environment.

Arguably more important from a U.S. investor perspective is how such delistings happen. As noted, one of the features of the VIE structure is that the wholly foreign-owned enterprise owners actually have little to no say on what happens. By illustration, in July 2016, the founders of the Chinese internet security firm, Qihoo 360 bought out U.S. shareholders at $77 a share, valuing the firm at $9.3 billion. While only 21 percent of minority shareholders voted in favor of the deal, Qihoo's chairman and president together controlled 61 percent of the voting power.

The company relisted in February of 2018 at evaluation of more than $60 billion. Qihoo's chairman personally made $12 billion upon the relisting. More than a total value of the buyout he offered 18 months earlier. Even this is not the worst case scenario. While it remains the most likely way these delistings play out, it's not inconceivable that the Chinese owners of the company could pay U.S. investors nothing.

As mentioned, the VIE structure provides few rights or protections for U.S. investors. And the willingness of Chinese owners to pay is likely continent on what they expect to get out of it. However, there are some ADRs of Chinese listings in the U.S. depending on the details of the ADR contracts that would enable investors such as U.S. based global fund managers to convert those shares into corresponding securities listed on other overseas exchanges such as Hong Kong.

U.S. listed firms including Alibaba, JD.com, NetEase, Yum China, and New Oriental have already listed in Hong Kong. Today the vast majority of U.S. listed Chinese companies do not qualify for secondary listings on the Hong Kong exchange. And as such, U.S. investors in those companies would not be able to take advantage of this conversion or transfer process. U.S. investors advise securities of Chinese companies on overseas exchanges may likely be investing securities that are subject to weaker investor protections, including corporate government standards.

As mentioned earlier, it seems likely that President Xi would want to be seen as proactively calling companies home, rather than having them kicked off exchanges by U.S. regulators. That is the narrative for the Chinese citizens. We can easily imagine a parallel narrative for U.S. investors where the Chinese government blames in its view overzealous U.S. politicians and regulators.

COMMISSIONER GLAS: Mr. Das, this is Kim. I would just ask that you try to wrap up the remarks since we're a little bit overtime and then we'll get to the question and answer.

MR. DAS: The U.S. is in a difficult spot here as I testified earlier. And four years ago, I made a number of recommendations including increasing disclosure -- risk disclosures in Regulation S-K. And Chairman Gensler's focus on these disclosures, especially the VIE structure, I think should come as -- should be welcome and they are essential in order for retailer investors to understand how the VIE structure works and what they're in fact investing in.

Ultimately this matter has come down to one issue; China refuses to allow its companies to comply with U.S. inspections of their audits. At this point, the U.S. has made its decision and determined that they will insist on inspections as a condition of continued U.S. listings.

Having said that, this is not reason or grounds to disengage with the Chinese regulators on this issue. And further attempts to resolve this impasse through negotiations should continue.

U.S. regulators should as mandated implement the Holding Foreign Companies Accountable Act with all delivered speed. Without this leverage or the prospect of delistings, any negotiations certainly will not be fruitful. After all, listing on the U.S. market still holds

weighted prestige given that it remains the largest, deepest, and most liquid marketplace in the world. Thank you and I'm happy to address any questions.

PREPARED STATEMENT OF SHASWAT DAS, COUNSEL, KING & SPALDING

Testimony before the U.S.-China Economic and Security Review Commission

"U.S. China Relations in 2021: Emerging Risks"

September 8, 2021

Shaswat Das, Counsel, King & Spalding LLP

Introduction

My name is Shas Das and it is an honor to be presenting before this commission on the important topic of current U.S.-China relations. Before joining the private sector, I spent five years at the PCAOB in its international affairs department and more than 20 years in total working for the U.S. financial regulators. Among other responsibilities at the PCAOB, I served as the organization's chief negotiator with the Chinese regulators on cross-border cooperation and inspections of PCAOB-registered audit firms based in China. In this capacity, I worked closely with the SEC and U.S. Treasury Department. I should note at the outset that the views expressed here are solely my views and do not necessarily reflect the views of my colleagues or law firm.

This panel will touch on several issues. But I'd like to start with a 30,000-foot view of U.S.-China relations, which bears heavily on each topic. To that end, I will discuss *why* China is acting the way it is, sometimes in a manner that seems contrary to its own economic interests.

Many people in the U.S. tend to believe that people in other countries largely share our values. After all, we have successfully exported many aspects of our culture, including our innovative spirit and entrepreneurial drive.

While many have indeed embraced the pursuit of wealth, countries such as China, with a rich and varied history, do not fit so easily into the capitalist mold. It is through this lens that we are able to not only view more clearly the actions China has already taken, but gain a better understanding of why they have acted that way, and how they are likely to act in the future. In mid-August, for example, President Xi Jinping commented that Beijing will increasingly promote social equality, using the new catchphrase "common prosperity", in an attempt to portray China as a socialist country.[1] Despite this statement, China most definitely remains a communist country where property and economic resources are either owned or controlled by the state.

[1] Chong Koh Ping, *Chinese Stocks Slide as Beijing's Crackdown Shows No Sign of Abating*, Wall Street Journal, August 20, 2021

To skip ahead a bit, it is my belief that China has for the past several years viewed U.S. capital markets as a relatively easy source of funds. In light of the increased scrutiny of Chinese companies listed on U.S. exchanges, the most likely course of events is for China to retrench, forcing their companies to list on Shenzhen's ChiNext, Shanghai's STAR Market, in Hong Kong, or other non-U.S. exchanges.

Said differently, while China certainly cares about economic power, it also cares about issues such as pride, security, and most importantly control. They appear willing to sacrifice the monetary gains that accrue from U.S. listings if doing so will, in their view, better protect other values consistent with its authoritarian society.

Thus, any future negotiations regarding U.S. inspections of its companies' audits are likely to be unsuccessful without major compromises on both sides.

China's changing regulatory approach

China is quite clearly taking a more aggressive regulatory stance of late, with one agency in particular playing a very prominent role.

The most recent example is the actions taken against ride-hailing company Didi, with the Chinese government announcing an investigation into the company's data security practices, and then mandating the Didi app be removed from app stores, just days after the company raised $4.4 billion in a U.S. IPO. This has been followed by a new regulation that requires all companies with data on more than one million users—so effectively all internet companies—to seek formal approval from the Cyberspace Administration of China ("CAC") before pursuing a foreign listing.

The CAC has been around since 2011, but has only recently come to wield such outsized influence. It is governed by the Central Cyberspace Affairs Commission chaired by President Xi, and its recent prominence gives a sense of how seriously Xi is now taking data security (or perhaps more accurately, data control).

Other regulators include the State Administration of Market Regulation—basically the antitrust unit—as well as financial and trade regulators such as the China Securities Regulatory Commission, Ministry of Finance, and the Ministry of Commerce, which quashed Qualcomm's proposed merger with NXP Semiconductors in 2018.

Again, it is not so important *who* the regulators are, as what matters to them. And the recent elevation of the CAC sends a clear message that, for China, data security trumps financial gains. Or at least that is the message they want to send.

The reality, however, may be quite different. I generally believe this is all political/pretextual, rather than a genuine concern over data protection. With the prospect of delistings now on the horizon, the Chinese Communist Party ("CCP") has stepped up its scrutiny of Chinese companies listed in the U.S., largely in reaction to the actions of the U.S. government, including but not limited to the moratorium on new IPOs until such companies beef up their risk disclosures and separately the issuance of the Chinese Military-Industrial Complex list ("CMIC"). The CCP wants to control the narrative and be able to argue that they brought these companies back home on its terms, rather than because they were threatened with delisting by U.S. regulators.

Future of the VIE structure and potential economic consequences

Briefly, for those who do not know the history, the VIE structure was used early on by the Chinese internet companies Sina and Sohu, both of which listed on Nasdaq in 2000.[2] (It was also famously abused by Enron, which led to the establishment of new rules for the structure.) VIE stands for Variable Interest Entity, and is the primary method that Chinese companies use to get around rules that forbid foreign ownership of Chinese companies.

Put simply, the VIE is 100% owned by a Chinese individual, or in some cases such as Alibaba entities owned by Chinese individuals, usually but not always the founder and chairman. The shares sold to U.S. investors are part of a Wholly Foreign-Owned Enterprise ("WFOE") – which is the wholly-owned Chinese subsidiary of the offshore, shell company that is generally incorporated in the Cayman Islands or other offshore jurisdictions. In most cases, the VIE owns effectively all of the business through a set of contractual agreements, with the WFOE acting as a sort of "tracking stock" that fluctuates along with the underlying company's business, but which has *no claim on any significant business assets*. Presently, VIE arrangements transfer control to the WFOE, and indirectly to the offshore parent, which remains in the hands of Chinese nationals. The equity ownership of these companies is held by China-based shareholders; while the VIE shell companies have contractual rights, the enforcement of those rights is highly questionable.

Indeed, many prospectuses of these companies are replete with warnings about the lack of shareholder rights. Picking almost at random from the prospectus of electric-vehicle maker NIO, shareholders are warned they have "no general rights under Cayman Islands law to inspect corporate records or to obtain copies of lists of shareholders," that "it may be difficult or impossible for you to bring an action against us or against these individuals in the United

[2] Gillem Tulloch, "Variable Interest Entities in China," GMT Research, March 13, 2019.

States," and that "it will be . . . difficult for US shareholders to originate actions against us in the PRC in accordance with PRC laws."[3]

It is also worth noting that, while Chinese regulators have never objected to the VIE structure to any effect, they have also never blessed it. It is therefore *possible*—however unlikely it may seem—they could one day simply invalidate VIEs, leaving U.S. investors holding an empty bag. This scenario is difficult to imagine, given that such a step *would affect all foreign investors*, not just those located in the U.S., effectively cutting off Chinese company access to the global financial markets. Rather, it is far more likely that the Chinese government will tighten the rules for its companies listed overseas, including requiring companies that have personal data of users above a certain threshold to apply for a cybersecurity review to purportedly safeguard national security.

Convertability of ADRs and U.S.-listed Chinese companies that could "go private" or "go dark"

The future of the VIE structure leads directly to the question of how companies are removed from U.S. exchanges. As mentioned, while the VIE has been a useful construct for Chinese companies over the past two decades, much of the value from China's point of view has been the ability to evade measures such as U.S. audits of Chinese firms. Now that this is being threatened, the VIE structure holds far less appeal for China in the current environment.

As you may know, I dealt with this very issue during my time at PCAOB, when China showed little interest in complying with U.S. inspections, notwithstanding an agreement that was struck providing cooperation on cross-border investigations. But with the Holding Foreign Companies Accountable Act—and significantly, President Trump's Executive Order, as amended by President Biden, prohibiting U.S. persons from buying or selling certain, identified publicly traded stocks that finance the Chinese defense sector—the U.S. finally appears ready to stand its ground.

Arguably more important, from a U.S. investor perspective, is *how* such delistings happen. As noted, one of the "features" of the VIE structure is that WFOE owners actually have little to no say in what happens.

For example, in July 2016, the founders of the Chinese internet security firm Qihoo 360 bought out U.S. shareholders at $77 a share, valuing the firm at $9.3 billion.[4] While only 21% of minority shareholders voted in favor of the deal, Qihoo's Chairman and President together controlled 61% of voting power. In fact, confidential fundraising materials for the

[3] NIO ADS prospectus, sec. gov, 2018.
[4] Jesse Fried, *The Risky Business of Investing in Chinese Tech Firms*, Harvard Law School Forum on Corporate Governance, February 4, 2019.

privatization—at the time of the deal —projected a 500% return by 2019, but even this proved conservative: the company relisted in February 2018 at a valuation of more than $60 billion. Qihoo's chairman personally made $12 billion upon relisting, more than the total value of the buyout he authored 18 months earlier.

Even this is not a worst-case scenario. While it remains the most likely way these delistings play out, it is not inconceivable that the Chinese owners of the company could pay U.S. investors *nothing*. As mentioned, the WFOE structure provides few rights or protections for U.S. investors. And the willingness of Chinese owners to pay is likely contingent on what they expect to get out of it.

In the case of Qihoo, the founder and corporate insiders, were clearly expecting to relist on a U.S. exchange relatively quickly, and so did not want to entirely burn their bridges. But if China is really turning inward and away from U.S. capital markets, we have to ask the question: What obligations do they have to pay U.S. investors anything at all? This is particularly true given the U.S. legislation requiring PCAOB inspections or face delistings, which could provide a ready-made scapegoat for Chinese regulators.

However, there are some ADRs of Chinese listings in the U.S., depending on the details of the ADR contracts, that would enable investors, such as U.S.-based global fund managers, to convert those shares into corresponding securities listed on other overseas exchanges, such as Hong Kong.[5] U.S.-listed firms including Alibaba, JD.com, NetEase, Yum China, and New Oriental have already listed in Hong Kong; to date, the vast majority of U.S.-listed Chinese companies do not qualify for secondary listings on the Hong Kong exchange, and as such U.S. investors in those companies would not be able to take advantage of this conversion or transfer process. Despite the lack of PCAOB inspections, U.S. investors that buy securities of Chinese companies on overseas exchanges may likely be investing in securities that are subject to weaker investor protections, including corporate governance standards.

I agree with something Carson Block—a short-seller with significant Chinese experience—recently said: "If Chinese companies largely get out of the US before the mandate to delist kicks in, then it kind of looks to Xi's domestic audience, like Chinese companies left the U.S. out of strength, as opposed to being thrown out."[6]

---

[5] The Economist, Buttonwood, "*How the delisting of Chinese firms on American exchanges might play out",* August 14, 2021.

[6] Akiko Fujita, *Why China is Cracking Down on certain publicly-traded companies, according to Carson Block*, Yahoo Finance, August 7, 2021.

As mentioned, it seems likely that President Xi would want to be seen as proactively "calling companies home" rather than having them kicked off exchanges by U.S. regulators. But that narrative is for Chinese citizens. We can easily imagine a parallel narrative for U.S. investors where the Chinese government blames, in its view, "overzealous" U.S. politicians and regulators.

Hong Kong's role in China's enforcement and regulatory approach

Finally, Hong Kong plays a large role in any U.S. delisting of Chinese stocks. Indeed, certain Chinese companies such as Alibaba already trade on the Hong Kong market, and for institutional investors it is a relatively simple matter to buy there as opposed to the U.S.

That said, while the Hong Kong market is indeed more liquid and "legit" than for example ChiNEXT, it is no Nasdaq. The U.S. dollar volume of daily trading in Hong Kong is somewhere around $25 billion, as opposed to about $200 billion on Nasdaq. Moreover, the Hong Kong market remains effectively off limits to many U.S. investors, either through lack of brokerage options to trade there, or simple unwillingness to venture outside the U.S. due to concerns relating to transparency and regulatory oversight.

Said differently, the Hong Kong market is a relatively poor substitute for U.S. markets. While many Chinese companies could and indeed do list there, a mass migration of listings to Hong Kong would limit access to some U.S. investors and, by extension, fresh capital from new offerings.

Recommendations

The U.S. is in a difficult spot here. Millions of U.S. investors now hold positions in what they believe to be claims on Chinese corporate assets, but which are in reality nothing more than shell corporations. Delisting these companies will almost certainly result in large losses for many U.S. investors, if not a total wipeout of their capital.

That said, ignoring the problem is likely the worst option. As you know, I fought hard to reach an agreement whereby China-based audit firms registered with the PCAOB would comply with U.S. inspections during my time at the PCAOB.

When I appeared before this commission four years ago, I made several recommendations about how we could potentially work with the Chinese government to resolve this issue. Obviously, during the intervening period, a lot has changed. China seems content to continue to tap U.S. capital markets for funds so long as we play by their rules, in many cases providing worthless paper in exchange for dollars, and not allowing their companies' auditors to submit to PCAOB inspections required of all other companies traded on U.S. exchanges.

In addition to modernizing and enhancing certain financial disclosure requirements in Regulation S-K,[7] in my earlier testimony, I argued for greater disclosure of the risks presented to U.S. investors. In this vein, I support Chairman Gensler's focus on more robust disclosures relating to investing in Chinese companies, especially the VIE structure, both with respect to new Chinese IPOs as well as filings by companies with significant China-based operations.[8] While the cornerstone of the U.S. federal securities law is disclosure, this alone, of course, is not a panacea when it comes to this matter – as has been well-established.

Ultimately, this matter has now boiled down to one issue: China refuses to allow its companies to comply with U.S. inspections of their audits, and the prospect of this changing seems bleak despite some recent reporting that China's State Council is ready to increase its efforts on cross-border audit cooperation during the latter part of this year.[9] The U.S., therefore, has a decision to make. We can either allow China to continue to play by its own set of rules, or stand our ground and insist on inspections as a condition of continued U.S. listings. That decision appears to have been made.

While this is no reason to disengage with the Chinese regulators on this issue, and further attempts to resolve this impasse through negotiation should continue, U.S. regulators should, as mandated, implement the Holding Foreign Companies Accountable Act with all deliberate speed. Without this leverage, or the prospect of delistings, any negotiations certainly will not be fruitful; after all, listing on the U.S. markets still holds weight and prestige given that it remains the largest, deepest, and most liquid marketplace in the world.

Thank you for the opportunity to appear before you here today, along with this distinguished group of panelists.

[7] SEC.gov | SEC Adopts Amendments to Modernize and Enhance Management's Discussion and Analysis and other Financial Disclosures

[8] Paul Kiernan, *SEC to Set New Disclosure Requirements for Chinese Company IPOs*, Wall Street Journal, July 30, 2021.

[9] Jonas O. Bergman, *China's Top Policy Makers Signal Plan to Fix US. Audit Impasse*, Bloomberg, August 23, 2021.

COMMISSIONER GLAS: Thank you, Mr. Das. And thanks to all of our panelists. I know we're a little bit over on time, so Vice Chairwoman Cleveland, if you wouldn't mind, I'm going to hand the mic back to you. And look forward to hearing further from our witnesses on some of the key questions.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Wong.

COMMISSIONER WONG: Thank you. My question's for Mr. Das. Thank you for your testimony. You know, you mentioned that the U.S. is in a tough spot on how to handle this issue of Chinese companies not abiding by its standards and being transparent. But my question is are we really in a tough spot? I can understand why an investor in these VIEs and in these Chinese companies would be in a tough spot. They don't want to see their wealth perhaps diminish by greater regulations in some sort of dispute between the United States and China.

But if you're a U.S. policy maker, if you're a U.S. regulator, being tougher, taking an enforcement action, delisting one or two companies, even if that has, you know, a diminishment of -- or systemic effect to diminishing the value of these listings, those listings only collectively represent, I think roughly 3.7 percent of all the listings on U.S. exchanges. All of those shares are not all held by U.S. investors. There will be some time for investors to make decisions on where to move their capital. And as far as a healthy market, that seems to be the proper decision. Putting aside the interest of individual investors, the interest of the U.S. in advocating and facilitating a transparent market seems to be a pretty easy decision. Am I wrong?

MR. DAS: Yeah. No, I would probably beg to differ. I think it's going to be -- it's a very challenging issue. If it was an easy one, I think the PCAOB and the SEC collectively would have decided to delist these companies years ago. I think they recognize the attraction by U.S. investors to Chinese listings, Chinese stocks.

As far as its percentage of the global market cap or actually the U.S. market cap, I think it's more around 6 or 8 percent. So we would see about $2 trillion go out the door. And there are many Chinese IPOs in the pipeline here. And you know, it's not just -- clearly we're concerned about retail investors and their lack of knowledge of what they're investing in, but it's the big institutional investors, the global fund managers and hedge funds and pension funds, endowments -- university endowments that invest heavily in Chinese stocks and have been rewarded significantly over the past decade or so.

So they clearly are not going to want to see these companies, you know, leave the U.S. markets and migrate to other exchanges, which will, you know, I think happily accept them. So I do think if it was, you know, if it had a marginal impact if you will, on the U.S. economy or the U.S. markets, the U.S. would have made that policy decision a while ago.

COMMISSIONER WONG: I mean what I'm saying is, you posit that the full delisting en masse of Chinese companies or VIEs would have a significant impact on the U.S. economy, which I think is right. What I'm saying is an individual enforcement action against one, perhaps two entities that are not abiding by the audit or transparency standards obviously would have a systemic effect. But its demonstration effect of what enforcement on a broad scale could be, that gives an opportunity and time for investors to move their capital out of Chinese companies. It gives time for Chinese companies in the Chinese government to rethink their compliance. And furthermore, I would say that yes, the idea that these companies simply can go to other exchanges internationally is an argument, but I think it's a facile argument. The reason the Chinese companies want to go to the U.S. as you know, in our markets is our liquidity -- the size

of the markets, the sophistication. So we have leverage here. Why can't we take individual enforcement actions?

MR. DAS: I think we can and I think it's been a collective reticence to do that. But there is some history here, not directly with respect to the Chinese companies listed here, but the actions that the SEC took against the big four accounting firms in China for failure to provide audit work papers relating to ongoing investigations. I think you may, you know, are likely familiar with that. And indeed a settlement was struck and fines were imposed -- very modest fines. So actions were taken, but ultimately they really didn't have the intended, you know, effect. It was a sunset provision there, so after, you know, four years the compliance obligations of these firms ceased.

So I still -- as far as taking, you know, selective enforcement actions against, you know, one of the largest or a few of the largest Chinese companies by market cap here in the U.S., I mean certainly, you know, that could be -- that could be done. But you also have to, you know -- it would be I think the basis of it frankly, would be the fact that they don't comply with, you know, PCAOB inspections. As far as their disclosures, I think, notwithstanding the fact that disclosures are being audited as we speak by the SEC staff, there is disclosure in all of the prospectuses about the risk of investing in these Chinese companies and the VIE structure that I discussed.

So I believe that the Chinese are already responding to the prospect of delistings. So they are -- you know, I think this is -- this is what I said in my remarks that they have now elevated the CAC, an agency that was effectively dormant for the last, you know, decade, and to impose cyber security reviews and place increased emphasis on data security, I mean as we all know, there's no requirement in order to list on a U.S. exchange that you, you know, disclose such proprietary -- or as the Chinese would view, its states secrets as part of the listing process.

So I do believe that's a red herring and really masks the true intension of the Chinese. And that is I think they see that the U.S. finally is calling their bluff. And saying that, you know, we are going to take action. But if you just do it against one or two companies, that still again may not have the intent effect. I mean of the $2 trillion, I would think, you know, most of that market cap is probably in about, you know, 30 companies -- maybe 35 companies. Of that, you know, we're talking ten state-owned controlled. And then the Alibabas and the Baidus and Tencents, and the JDs of the world here.

So certainly that would send a message here, but I think that the approach that the legislation is taking and now is being implemented by the SEC is the right approach going forward. And as far as to your point about leverage -- and I think that's probably where you're getting at, if you bring a few enforcement actions, you know, maybe the other companies will fall in line.

I think at this juncture, we do have leverage. When I was the PCAOBs chief negotiator for five years, I didn't have that leverage. I mean occasionally we would get a letter from Congress about this issue, but very occasionally. And when I was, you know, embroiled in negotiations in Beijing and pulled out the threat of these firms being deregistered, that really didn't carry a lot of weight at that time. So we're living in a different environment today.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Wessel.

COMMISSIONER WESSEL: Alright. Thank you to all three of our witnesses. I want to double down on Commissioner Wong's question and actually maybe even look at it more -- a new regime if you will to help advance compliance, but also to address what I think is, you

know, the inappropriate flow of U.S. funds to Chinese entity lists, military companies, and otherwise.

You know, Shas, you talked about the VIE is something that this commission has spent a lot of time on over the years, as well as lack of disclosure. All of which, you know, run counter to the Securities and Exchange Act and how we view markets.

I'd like to get first Mr. Harris, then Shas and our other witness thoughts. It seems to me that we're subsidizing the CCP with trillions of dollars of capital in some ways, but also tax payer money. What would you think -- again first, Mr. Harris, of identifying certain issues that are at risk; VIEs for example or those companies not complying with the U.S. transparency standards and eliminating capital gains and loss preferences, as well as treating any capital gains as ordinary income? Together those tax expenditures amount to billions of dollars, which now are going to subsidize investments in Chinese entities that aren't conforming with U.S. standards. Mr. Harris? You're on mute.

VICE CHAIRMAN CLEVELAND: You're muted, Mr. Harris.

MR. HARRIS: I think that would be a good start, but only a start. In litigation, there's a saying that you never fund your enemy. We are right now funding China. And there's a real tension out there in a lot of areas between what's good for businesses -- in particular, big businesses -- and what's good for the United States. And I take the position that Chinese companies on U.S. exchanges are in the long run at minimum very bad for the United States. And so I would advocate at a minimum that Chinese companies be forced to comply with all the requirements that other companies are forced to comply with.

On the issue of disclosures regarding VIEs, I defy anyone to talk with investors to see if any of them really understand VIEs. Because I have yet to talk to anyone but lawyers who deal in this who truly understand VIEs. Our own clients constantly do not even realize who they're doing deals with when they're doing deals with these big Chinese VIEs. An example I always give is Alibaba. We'll say to a client, who's the entity on the other side? And they'll say Alibaba. And we'll say no, it's not. Alibaba is some company in the Cayman Islands. What's the entity? People do not understand what's going on. Disclosures are not necessarily going to help that.

We've had so many companies from China that have been delisted for basically lying about their balance sheets. I'm not so sure that the American investors wouldn't be better off with no Chinese companies as well. Now obviously there would be short-term repercussions from that, but it's time that we really decide what we're going to do and how quickly we're going to rip off that Band-Aid.

COMMISSIONER WESSEL: I agree. You know, I'm happy to rip off the Band-Aid. But again, I think there's several different ways of doing it. Limiting investments in entity lists or CMCC companies, delisting companies which don't abide by our rules in full measure. But the other investments which could be made on other markets, eliminating capital gains preferences both loss and gains so that the U.S. tax payers are not underwriting those.

MR. HARRIS: That all makes sense to me.

COMMISSIONER WESSEL: Thank you. My time is up.

VICE CHAIRMAN CLEVELAND: Senator Talent.

COMMISSIONER TALENT: Thank you and thanks to the three of you. I really looked forward to this panel and you've been very helpful. Mr. Das, I really was intrigued by your theory that the reason they're -- one of reasons they're doing these tech actions is so that they look like they're calling their companies home, not being forced home.

But I'm going to just triple down a little bit on what my two colleagues have said and get your reaction to this. I focus mostly on the security end of the issues that we do here. I mean there are others here who are experts in both who are in finance or business. But I do as a -- you know, as a person who was in public life and a representative in different legislative bodies for 20 years, I'm really concerned -- I would be really concerned that my constituents who are investing in these companies have no idea the amount of risk that they run.

And I say this from a security angle and then you all comment please. I mean what we're -- I mean in the highest sense, what we have here between the United States and China is a growing conflict between a rising hedger fund and an established hedger fund who define their vital national interests in mutually exclusive and contradictory ways. Now nobody in the national security community in the United States wants or is hoping that this is going to result in kinetic conflict, although the chance of that is growing.

But I will just tell you, I don't think for the Wall Street and the investment community to be going on month after month thinking this is a question of let's find this great return on this IPO for our clients, I just -- I don't think they're dealing in the real world. I think this mutual economic, you know, investment and the rest of it is going to end and could end any time. And I would not want my constituents to lose their shirts.

So that's all I have to say. I mean I just think we've got to -- we've got to wake up and smell the coffee here. I'm not ranting at you all because I think all three of you understand this. But tell me, do you think that the people -- you know, the kind of people -- and I'm just from Missouri, I don't see these people all the time -- but can people who run the big firms in Wall Street and the hedge funds, do they really get this -- What's going on? What could happen here? That's my question. (Simultaneous speaking.)

MR. DAS: I'm happy to reply.

MR. HARRIS: I'm sorry.

MR. DAS: Many of them get it. Many of them do not. Many of those who get it, do not care. Their view is there's money to be made. Shut up. Let's keep going. Then there are those who don't get it. And it took an investment banker to explain to me how it is that these very smart people don't get it. And his explanation was that we are trained to look at companies and industries. Very few of us look at the big picture like governments, like conflicts, like what's going on in terms of China essentially moving farther along the path to the various stages of communism.

COMMISSIONER TALENT: Yeah and I -- we only have a minute and a half left. Look, I don't -- for national security reasons, I think we need to stop funding them. I mean as I said when I briefed some of my former colleagues last year because we had an investment chapter then, I just for once -- you know, I said for once, let's not sell our enemies the rope they're going to use to hang us. Just once, let's not do that. Okay?

But the other issue is again, I just don't think investors particularly passive and retail investors, I don't care whether they read the notice in the VIE perspectives or not. I just don't think they understand how volatile this situation is. This is an instance where we really need to protect them a little bit from themselves.

Thank you, Mr. Harris. If anybody wants to comment, they can.

MR. DAS: Yeah, I'll comment here. I mean I share your concerns. I mean clearly the retail investors often and generally do not understand the VIE structure. You know,

notwithstanding all the, you know, disclosures that may be provided in SEC disclosure filings. Either they don't read them or it's also, you know, a very complex structure.

So I recognize that, but by the same token, many of these retail investors gain their investment exposures to these Chinese companies through the big mutual funds. Right? Through you know, hedge funds, 401(k)'s, you know, through various investment vehicles. And are relying on the investment advisors and managers, you know, who are functioning as fiduciaries here. So as far as do they get it? I think they do. But they see it as a proposition of high risk, high rewards. And so far, it's been high rewards for them.

COMMISSIONER TALENT: I understand and I'll wrap it up. I do think they began doing all this in the context of a Sino-American relationship that was very different on both sides.

MR. DAS: Right.

COMMISSIONER TALENT: When the United States was about engagement and they were about hiding and biding. And I think that ended about five years ago, really in the Obama administration a little more than that. And I just don't think the community has caught up with it, but thank you.

VICE CHAIRMAN CLEVELAND: Commissioner Scissors.

COMMISSIONER SCISSORS: Thank you. I'm going to start with a complaint. People should stop talking about market capitalization of Chinese firms listed here. We don't care unless you're the New York Stock Exchange and the NASDAQ. We care about the exposure of U.S. investors, which is considerably less than market capitalization. The Wall Street Journal loves to throw around the market capitalizations. And you can't touch this money, it's so big. But they're exaggerating, they're doing it knowingly.

And in particular with regards to Mr. Dawson's comments, the firms that know better and claim this is a high risk investment, we have no obligation to protect them. Right? We may have an obligation to protect the retailer and past investors you're talking about, but we do not have an obligation to protect Goldman Sachs. If they say oh, no. How could you possibly put our money in jeopardy here? Well you got into a high risk, high return investment. And you understood the situation or you claimed to. That's just a complaint.

My question is actually for Ms. Fair, which is we have a lot proposals for gathering information, which are understandable because the Chinese do a lot of information gathering and we don't seem to. And we have a lot of people who want to learn more about China including our clients in the Congress. And they would love to like push a button and there's all the China information that they want. Nice, not really realistic. Could you say more about your proposal? Flush it out? The idea I endorse, but as an idea, it's not really useful as a policy recommendation without more on the bones.

MS. FAIR: Yeah, of course. Thanks for the question. I leave the legal framework and organizational structure to the experts. But my background is running this company where we collect, aggregate, and analyze mission critical information gives me some perspective.

I imagine the clearinghouse could build on or help augment the work already being done by the National Economic Security and Financial Intelligence Executive, pulling that information together. It could work as a central point to understand that evolving threat landscape. I think different elements of the U.S. government have access to different types of information relevant to this challenge. And its information that we don't usually think about in the national security context.

To the Senator's comment earlier, I think this is somewhere we haven't been thinking about it in this context before. And to your comment that people previously have not been thinking about it that way. So information that is out there and needs to be organized in order to see the insights of what's going on could be helpful.

So things like information that the SEC has for example or Department of State of the U.S. Trade Representative. So pulling that information together so that we have some more accurate data on what Chinese companies are actually doing, where they're doing it.
And we have some longitudinal data. So a lot of the stuff that we see that comes out is one-off reporting. And it's often used out of context or it's used to make a point. And China plays the long game. And you can see the longer, sort of data stream that you have, the more you can see these trends and dynamics emerging. So I think it's an issue of pulling together economic and financial data and putting it or looking at it through a national security lens is a newer sort of approach to pulling together that information.

COMMISSIONER SCISSORS: I yield back the rest of my time.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Kamphausen.

COMMISSIONER KAMPHAUSEN: Thank you especially to Mr. Harris and Mr. Das. Mr. Das, your testimony -- your written testimony was especially helpful when helping me. Like Senator Talent, I come from a national security background. And so it's clear for the first time how these issues are not separable from your testimony. And I want to lead you to maybe talk about a worst case scenario and then what happens.

But if I understood your testimony correctly, the VIE structure is a problem. The Chinese government, the CCP may have kept it at arm's length, but it's allowed it to exist. They might not have understood the implications of what the VIE structure might mean in the temporary content, but that's one piece.

The second piece is its linked is the access to auditing papers. And you say in your testimony that's never going to happen -- or you come close to that, so you can correct my over statement if I've done some reading your reading your facial language for people who can't see Mr. Das. The risk of course is that U.S. government actions or CCP action that result in either the companies coming home or the delisting can have a catastrophic effect on the value of the investments, whether they are individual retail investors or the large institutional investors who if Mr. Scissors is to be believed and usually we do, there will be actors in this charade.
So what's the worst case? Right? What I worry about is I'm all for ripping off the Band-Aid, but which one? And what timing? And then what happens? We could say well that was the risk that the investors took in investing in these companies, but that's a really -- very simplistic in my view, assessment of what happens next? So what's the worst cast? And then what happens next in your view?

MR. DAS: Well, in terms of the worst-case scenario, U.S. investors effectively could be bought out by the Chinese insiders of these companies -- the operating companies at a very low valuation, go dark or go private, and then relist elsewhere outside of the U.S. at a much higher valuation. Obviously, this will, you know, result in tremendous losses to U.S. investors, particularly the retail investors. But as I noted, there are some ADRs that do allow for the transferability of the shares assuming they're listed on another exchange such as the Hong Kong Exchange.

And you know, there are threshold requirements in order to list on the Hong Kong Exchange. And so that generally means it's going to be the largest Chinese companies. So for

the institutional investors, they can -- you know, in many cases, they can transfer or convert their U.S. shares, you know, into the shares in Hong Kong.

So I think the impact on them would be less severe. But overall in terms of millions of investors, again you know, focusing on retail investors who I think have been aptly stated here or stressed, really don't know what they're investing in, which is effectively a shell company. They're going to be hurt, but at this juncture I do think that the administration is taking the right steps here. And there was reference to the entity list, but I think more, I think relevant to this issue is the -- I guess formerly the Chinese Communist Military List, but now the CMIC list. I mean that is a harbinger of things to come. And of course with the legislation, the Hold Foreign Companies Accountable Act being passed last year and being implemented, I mean, I think this is finally -- you know, we're proceeding on the course of action that we need to.

And to your, I guess, initial statement that -- I think I did shrug -- but when you said that it was impossible that a deal could be struck in terms of access to audit work papers, sorry to be a lawyer here, but I think it's -- I think it's unlikely, not impossible, but if it's going to -- if a deal is in the works or should I say to be negotiated, having the leverage of possible delistings, I don't this we can use "impossible", I think the legislation going forward of delistings is absolutely necessary. We need that leverage. Leverage that I did not, you know, have, you know, six years ago when I was negotiating with the relevant regulators.

So I do support, you know, the administration's stance here, what they're doing, the legislation. Moving forward, the rule making will be completed by year's end and next year will be the first non-inspection year and start the clock ticking. So I don't know if that answers fully your question, but thank you very much.

VICE CHAIRMAN CLEVELAND: Commissioner Goodwin.

COMMISSIONER GOODWIN: Thank you, Vice Chair Cleveland and my appreciation to the panel. Again Mr. Harris, I wanted to ask you a question about the lack of understanding in the investment community of the VIEs and you used the Alibaba example. I read one commentary -- it might be dated now -- that actually suggests that our accounting rules might be exacerbating some of the problem and the lack of understanding and appreciation for this structure.

A gap allows -- it's my understanding VIEs to consolidate their financial statements with that of the underlying Chinese domestic companies. So that when even those sophisticated investors do look up what they think is an Alibaba share, what they're actually seeing, limited though the information may be, are the balance sheets and the income statements of that company and not the shell company in the Cayman Island. So what sort of changes can we look to in our own accounting rules that might help address this issue?

COMMISSIONER GLAS: Mr. Harris, you're on mute.

MR. HARRIS: I'm sorry. Unfortunately my knowledge of accounting standards in this issue is not deep enough for me to even be able to answer that question.

COMMISSIONER GOODWIN: I'm sure they exceed mine(Laughter). Well, anyone else on the panel want to take a stab at that?

MR. DAS: Yeah, I mean in terms of the VIE structure, it actually, you know, ironically has its roots with Enron in the SPV vehicle that Enron used. And there is a deep irony there. And it was allowed both by China and the U.S. I mean I think, you know, one thing that we could change is, you know, the allowance of the dual class voting share structure, which is frankly the reason why Alibaba conducted its IPO here in the U.S. back in 2014, rather than

Hong Kong. Now they're able to conduct a secondary listing in Hong Kong because Hong Kong has relaxed its own rules there.

So there is clearly, I think, changes that can be made from an accounting standpoint that I think, for many of these companies that list here and the means by which they do so. I will say that, I mean, the VIE structure has been around for a long time. It's not unique to or specific to Chinese companies. It's been used by other companies located in other countries. But you know, clearly the Chinese have used it to the greatest extent here. I'm not sure if that --

COMMISSIONER GOODWIN: Thank you.

MR. DAS: Okay.

VICE CHAIRMAN CLEVELAND: Does that complete your questions, Mr. Goodwin?

COMMISSIONER GOODWIN: It does. Thank you, Vice Chair.

VICE CHAIRMAN CLEVELAND: Commissioner Glas.

COMMISSIONER GLAS: Thank you so much. And I understand we got a note from Mike Wessel that Jeff lost his connection. So I know Mike has been given a question by Jeff so after I go.

I appreciate the testimony here today. Mr. Harris, I really appreciated your comments about some of the advice that you give to your clients about the complicated nature of doing business in China, whether related to legal matters or other matters associated. And some of the advice -- and I don't want to paraphrase what you said -- so please clarify if I've got this wrong is you know, folks should sort of cease doing business in China or try to extricate themselves out of China into other market places and the difficulties associated for companies to do that.
So what is your advice to U.S. businesses that you're dealing with on a daily basis that say I'm going to be doing business in China after the foreseeable future of how they protect themselves? And how investors can protect themselves right now?

And for any our panelists, is Congress giving this enough attention? When I heard Commissioner Wessel's comments about potential solutions and then Senator Talent, it made me think that there has not been enough attention maybe in your worlds because -- or in our worlds where we're examining some of these issues. But what could we be doing to provide more attention to some of the risks associated for people who may unwittingly not know how their investments are at risk?

MR. HARRIS: Excellent questions. Can you hear me?

COMMISSIONER GLAS: Yes.

MR. HARRIS: Yeah okay, alright. So what I find interesting is how businesses react to risk. When President Trump initiated the tariffs we started talking to our clients saying this is the beginning of what we see as the decoupling between China and the United States. And literally only one client believed us. And it was not until President Biden became President and did not roll back the tariffs that businesses started realizing en masse that the tariffs looked like they were here to stay.

Most small and mid-sized business are too busy scrambling to deal with long-term risk. But with all that has gone on in the last few months, they are really starting to deal with the tariffs, the increase in shipping costs, the inability to go to China reportedly because of COVID, China cracking down on businesses left and right. Our clients are starting to see it. They're trying to figure out what to do. It's very difficult.

As I mentioned, there was a period of about two weeks where I must have asked about 15 of our clients that manufactured in China, whether they wanted to get out. And they all said yes. And then people say well how can that be? Why don't they just leave? Well it's definitely not

that simple. A number of our clients have no idea how to get out. And we refer them to people who can help them move their production to Mexico, to Thailand, to Vietnam, et cetera. But the reality is, is China is amazingly easy. They have the best soft infrastructure in the world in terms of helping manufacturers by far. Nobody comes close. So there's no one substitute for China.

So it's difficult and often times it's expensive, and sometimes it's impossible. And other countries are doing a better job than the United States in terms of helping their companies get out. Australia and Japan for instance subsidized their companies to move their manufacturing back. The United States does not really do that.

The tariffs in particular are in some ways broad, but in some ways sloppy and random. Meaning that in my view, they disproportionately negatively impact small and medium sized companies. Now that tends to be our client base, so that's who we hear from. But we have had companies that have gone bankrupt or had to shut down because of the tariffs and it seems like a lot of the exclusions from the tariffs go to very large companies that if they needed to, had the in-house capability and the money to move out. So I would like to see some changes there.

In terms of what companies can do that keep doing business with China, I won't go into it because that would be my -- I do a webinar on this and it takes an hour. But basically, not much has really changes in that respect. They need to be careful. They need to do -- They need to do whatever they can to protect their IP. They need good contract, just basic stuff. That really hasn't changed.

COMMISSIONER GLAS: Thank you so much, Mr. Harris.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Wessel, are you prepared to ask a question?

COMMISSIONER WESSEL: I am, thank you. And this is for Mr. Harris. Commissioner Fiedler asked whether you agree with BlackRock that U.S. investors are like on China investments and should be investing more. I believe they indicated that they should be trebling their investments. What are your thoughts?

MR. HARRIS: Well first off, my older brother is a very successful stockbroker and he'd probably be better at answering this than me. All I will say is that I've had an interest in the market for a long time. And I even invested in Russian stocks when Boris Yeltsin got rid of, I believe it was his fourth Prime Minister. So I'm willing to take risks, but I have never put a penny in a Chinese company. And I ascribe that as being hit over the head too many times by reality. I view it as a very high risk investment.

I know BlackRock knows a lot more about investing than I do. And it may be a good high risk investment, but I think people should view it as a high risk investment for the reasons that have come out today.

COMMISSIONER WESSEL: I see Commissioner Fiedler is back online. Jeff, would you like to follow up?

COMMISSIONER FIEDLER: I just caught the last bit of your answer, but I get the gist. I just have a question, do you think there are any red lines major U.S. investors won't cross to invest in China?

MR. HARRIS: Yeah, potential losses.

COMMISSIONER FIEDLER: Yeah, but we're talking about potential losses right now.

VICE CHAIRMAN CLEVELAND: Jeff, we couldn't hear you.

MR. HARRIS: I think he said there are potential losses right now.

COMMISSIONER FIEDLER: Correct, yes.

MR. HARRIS: Well there are, but I think that companies like BlackRock who they were wrongly criticized by George Soros who knows a lot more about investing than I do. But there are still plenty of companies out there like BlackRock who apparently viewed the rewards as exceeding the risks. And you know what? They might be right. They might be right for the next year or the next three years or the next five years. Who knows.

COMMISSIONER FIEDLER: So for instance, BlackRock now as a U.S. company is circumscribed from offering to U.S. investors, Chinese military-related companies. When it opens up a wealth management operation in China, presumably it is not circumscribed because those customers are Chinese. Is that correct?

MR. HARRIS: That would be my thought, yes. And that also might be a reason why BlackRock is encouraging Chinese investments because BlackRock may be making a lot more money by being on the good side of China than being on the bad side.

COMMISSIONER FIEDLER: I mean basically though in the BlackRock case, it's not BlackRock's money. Right? It's their individual clients' money --

MR. HARRIS: Correct.

MR. HARRIS: -- pension fund money, 401(K) money -- (Simultaneous speaking.)

COMMISSIONER FIEDLER: Okay, thank you.

MR. DAS: If I could add with respect to BlackRock operating in China, you are correct. They're able to manage the funds of Chinese citizens and that would not run afoul of U.S. law. Specifically --

COMMISSIONER FIEDLER: At the moment.

MR. DAS: At the moment, yeah.

COMMISSIONER FIEDLER: Frankly I don't see that expanding. I don't see the administration expanding to the CMIC list.

MR. DAS: We'll see.

COMMISSIONER FIEDLER: Yeah, we'll see.

MR. DAS: I don't mean in terms of entities, but I mean in terms of U.S. investment managers providing advisory services to non-U.S. persons.

COMMISSIONER FIEDLER: Thank you.

VICE CHAIRMAN CLEVELAND: Commissioner Borochoff.

COMMISSIONER BOROCHOFF: Thank you very much. I'm going to have a question for Ms. Fair in a moment. But I want to just comment because it's so close to home.
I spent an enormous amount of time from 1997 until 2001 in meetings -- various meetings with Ken Lay and his President, Jeff Skilling. My company did work for them and starting in about 1998 or '99, they stopped paying me. And it was always later and later and later.

People all over America thought that Enron was a great company, super strong. In the year 2000 after the presidential election, there were many talks about Ken Lay who retired so that he could be appointed to the Cabinet for the President. The President did not appoint him and less than a year later, the company went broke and everyone lost their money. I lost my little bit they owed me. But thousands of people lost their jobs and their retirement. And the net effect to the economy was gigantic.

It is a true statement that when something ripples, even when it's small, but it has a big emotional issue, it really hurts the economy. One only need look at the World Trade Center and two buildings falling down and the effect that it had on the economy that year. And I lived through that like many other business people. It doesn't take a lot to disrupt our economy if there's an emotional attachment.

So I would say those special purpose entities, I asked Ken Lay about them one time because were telling me I should be investing in businesses instead of the ones I owned, which I didn't do. And he couldn't explain to me what they did because it was just too complicated, he said.

So having said that, I join with my colleagues who think that sanctions and greater enforcement are necessary on the VIEs. I view them as no really big difference than the special purpose entities that Sarbanes-Oxley worked so hard to straighten out. And even though it was very expensive, it had some great effect.

My question for Ms. Fair has almost nothing to do with that. But I'm fascinated with what you had to say regarding your AI format to track the influence peddling effectively online that's going on inside China. And I have two or three questions that are all kind of interconnected. But here's my primary one. What methodology are you using to do that? Without giving up some propriety thing, is it primarily tracking key words or is it key concepts? I'm trying to understand just in a general sense how you do that.

Then secondly I would ask, have you ever done that domestically to look at the kinds of influences that are coming through the internet today, both against companies and ideas? Because there's been a lot of talk for a while now about these sorts of influences occurring in America. And I would think that what you're doing over there probably needs to be done here.

MS. FAIR: Yeah, thanks for the question. So methodologically, all of our insights come from publicly available information. It goes back to the data comment. There's a lot of stuff out there. And we use a variety of things. Some of it is as simple as the Chinese government has accounts on all of the social media platforms around the world. We follow those. We follow them on Twitter and Facebook and all the other places, as well as on Chinese social media platforms.

So first and foremost, you can see just like we do here, what they are pushing or discussing. And then if you compare that to other bits of information that may or may not be true. Right? And what do they say? And how does that match with other data that exist in the open space about sort of truth, if you will.

Some of other techniques do follow things like key words. So if there's particular topics that folks are interested in, we can monitor those as well. Content moderation is pretty straightforward. There's a bunch of organizations that follow that; FreeWeibo, Free WeChat, Weiboscope, China Digital Times. They all have a variety of techniques that they use to identify content that's live for some amount of time. And then content that is no longer alive. And if you look at that over time and at scale, you can start to see what patterns of things are sensitive or not.

And as I mentioned in my comments, often these things are used in concert. So often some propaganda will be pushed out through the official channels and other content that is not in line with that may be removed. So does that answer your question?

COMMISSIONER BOROCHOFF: Yeah, I understand you're creating a rubric virtually. I got it.

MS. FAIR: Essentially a framework, yeah. As far as domestic, we do look at that as well. So looking at again, as I mentioned, Chinese government entities have accounts on western -- U.S. social medial platforms and other social media platforms. So looking at that content, what it matches, how it matches with what they're saying domestically. Sometimes it's the same. Sometimes it's different.

We also look in other countries. So they are messaging out to South America, to Africa, to Europe. It is a global push to shape the narrative around all sorts of things like for example, the things you've been talking about; the competitiveness or the attractiveness of our markets. And it's part of the array of things that they use while trying to influence where their companies and other companies might want to list or invest.

COMMISSIONER BOROCHOFF: Thank you, that's good. Thank you.

VICE CHAIRMAN CLEVELAND: Very helpful. Commissioner Bartholomew.

CHAIRMAN BARTHOLOMEW: Thanks very much and thank you to all of our witnesses. As I listen to all of this, I just think about how greed is an extraordinary blinder. It's just, you know, people are making all of these decisions with the expectation that they're going to be making a lot of money.

Mr. Harris, you had mentioned about a company saying they were just looking at companies and industries. And I guess I'm naive, but I always thought that access to accurate information in real time was a very important principle in business. So I wonder how even when companies are looking -- or the people you talk to are looking just at companies or industries, do they trust the data or the information that they're getting on the ground in China?

MR. HARRIS: No. No, I don't think any of our clients trust the data that comes out of China. And I think one of the problems -- you talk about greed being an issue. Another issue is success. I grew up in Michigan and moved to the West Coast and people always acted like General Motors and Ford should have seen everything coming. And I would always say to them they've been -- they were successful for 80 years. Our success breeds repetition. And companies are not good with change. There are all sorts of studies on this. And if you've done well in China or with China for the last years, you're going to tend to block out those who are saying that it can't be done.

CHAIRMAN BARTHOLOMEW: So let me ask of all of our witnesses a bigger question, which is that we have talked here a little bit about a risk to individual investors. We've talked about risk to company. And Mr. Harris, in some way, just listening I sort of differentiate the manufacturing companies from the investment banks that the hedge funds, private equity, all of that.

But I guess what I'm concerned about is systemic risk. You know, we have gone through situations where companies have said -- investors have said, we're too big to fail. And the U.S. tax payer ends up being on the hook for this. And I'm particularly concerned about the pension funds -- you know, the funds that are being invested. And so I wonder if any of you could talk to what you think some of the systemic risks might be of the BlackRocks, the Goldmans, all of these companies going (audio interference) into investments in China. Mr. Harris, do you want to start?

MR. HARRIS: Okay. Well I view -- I don't know that I'm qualified to talk about the systemic economic risk. What I view as one of the biggest -- what I view as an even bigger risk is China insinuating itself into the United States and doing it via businesses, getting our IP, doing it with spies, doing it by sending people over here to work for American companies or working for American companies in China. And there's a lot of naivete on that.

And our clients will say well, you know, I've been friends with Mr. Zhang for ten years. He would never do anything. And my response to that always is nothing against Mr. Zhang who I'm sure is a great person, but do you really think that when the CCP knocks on his door and says you need to give us this information or this data or this IP or your parents pension is going to be

cut off or something else very bad is going to happen, do you really think he's going to be able to withstand that?

And that's an issue that really troubles me. It troubles me in particular in the context of universities. Because my father was a university professor and I very much believe in academic freedom, but I know for a fact there are spies in U.S. universities and colleges. I talked with a company that actually monitors for spies in U.S. companies. And they say in a lot of respects, they're fairly easy to spot because they have a history of working for Chinese government companies, et cetera.

And this company said that they called up a university and said you have a -- I can't remember whether there was one or two -- they called up a local university -- spies in your X, Y, and Z department or departments. They were in the Sciences. And the university basically said there's nothing we can do. And so that to me is the systemic risk is the fact that there's this -- people talk about decoupling, but right now, there's a coupling. And it's a coupling that was not present during the Cold War with Russia. And I don't know how we handle that. And I certainly don't want to see a return to the way we handled it during World War II.

CHAIRMAN BARTHOLOMEW: The naivete of companies is always something. I mean having been doing this now for 20 or 30 years, every single company that comes -- you know, that we have contact with always believes that they are the one who has the key, right, to being able to (audio interference).

MR. DAS: Right.

CHAIRMAN BARTHOLOMEW: But I would like to get back to systemic risks if there's a chance. And again, I'm thinking about the "too big to fail" issues. Ms. Fair, Mr. Das, do you have any observations about that?

MR. DAS: Yeah, I'm happy to comment. I actually do know something about systemic risk given that I worked at the Treasury Department during the global financial crisis and including the development of the Dodd-Frank Act.

With regard to your concerns about whether, you know, some of these pension funds, which you know, the CalPERS of the world and many other large public pension funds that hold, you know, vast, you know, millions of assets, I don't see the same level of systemic risk there because I do think that these institutional investors -- and we've talked about it before -- they do know what they're -- what they're getting into. I mean there is a level of buyer beware there. You know, again as we discussed, you can have all the disclosures in the world, but you know, the big institutional investors, they know the risk involved. And you know, they tend to be generally very diversified. And that's something that they monitor closely. You know, they have to, you know, disclose their, you know, portfolios on a periodic basis. Yes, you know, they're focused on shareholder maximization. But given those risks, you know, they tend to have very, very diversified portfolios and will hedge those risks accordingly.

So I just -- and I don't see, you know, a too big to fail situation here, the likes that we saw back in 2008 and 2009. You know, granted maybe some people could draw similarities given that the big banks were, you know, selling these, you know, MBSs and other asset back securities that ultimately proved worthless. And you know, the credit default who obviously didn't provide adequate insurance protection. And so that -- you know, obviously that led to the Dodd-Frank legislation and higher capital requirements among, you know, many other prudential and supervisory standards and requirements.

But I just don't see that in this circumstance. I could be proven wrong, you know, in a few years. And if so, I probably will not be invited back to this --

VICE CHAIRMAN CLEVELAND: Oh yes, you will.

MR. DAS: -- but I just again -- I mean the way our securities law system works, I mean the cornerstone is really, you know, disclosure and enforcement. And so you know, when there are bad actors, yes. The SEC will go after them, whether it be from, you know, market manipulation or outright fraud.

But here I think with the institutional -- the big institutional investors; the pension funds, I generally think they know what they're doing. And they do understand the VIE structure and what they're getting into to.

VICE CHAIRMAN CLEVELAND: Alright, thanks very much. So I have a question for Ms. Fair, but I want to clarify one point with you, Mr. Das. Since the PCAOB was established and you were involved in that wrangling, is it accurate to say that there is no authority -- additional authorities necessary for the Security and Exchange Commission to act tomorrow -- setting aside the legislation that creates the three year runway -- there is no restriction, prohibition, or limit on the SECs ability or authority to act tomorrow to proceed with removing companies that fail to comply from our exchanges?

MR. DAS: Yes, that would be my understanding.

VICE CHAIRMAN CLEVELAND: Thank you. So the risks relates to whether its pension funds, institutional investors, or individuals, there's been a long runway. They have known for literally since PCAOB was set up and all the efforts were made to negotiate some type of transparency and good governance. We've moved into an area where, notwithstanding that law, we've created additional rules and legislative authorities to encourage the Securities and Exchange Commission to do what they already have the ability to do.

Turning to Ms. Fair, I'm very interested in following up on what Commissioner Borochoff raised. I'm interested in your methodology and we could talk about that all day long. I just had one question, which is as you examine what all of these government entities are doing on social media, I'm not sure how long you've been doing it, but I'd be curious what you see in terms of changeover time. Are we seeing an increase in focus on tech companies or are we seeing a shift to support Xi's third term so that any social dissatisfaction, whether its healthcare or education, we see those companies targeted? I'm just curious over time and now, what are we seeing in terms of trend analysis?

MS. FAIR: Yeah, so we've been following since about 2018 is when our data starts, so we have some good longitudinal data. I would say that there's sort of two types of changes. One is topic-related and one is methodology-related.

So I'll start with the second one because it's a big jump. So one of the things that we saw at the beginning of 2020 was almost a two fold increase in the amount of government content being pushed out online in the wake of COVID. Before that, we would get questions, what do you think the capacity is of the Chinese government to push out information? And we said well based on these, you know, two years of data, we think this. And overnight practically, they marshaled enough to double it right around February of 2020. And it's really remarkable in our data. And it has not gone down since then. It's backed off a bit, but they really doubled down on that information push and the information they're putting out into the information environment. So that's one sort of just general context.

In terms of themes, the themes are driven in some ways consistent over time and the individual events within a theme change. But you wouldn't be surprised that public health is a common one. That was true even before the pandemic. Certainly during the past six to 12

months, that was a higher one. We've seen that fall off to some degree, but it's still in the top eight or so of the things that they talk about or are focused on.

And one of the shifts we've seen in the past six months is away from public health in particular, sort of claiming that they have COVID under control. And more focused on U.S. and other countries lack of ability to control that. Or how U.S. -- the U.S. is or is not engaging in China or trying to engage in China. Or a lot about the elections and the events in January about evidence that this is more evidence that democracy is not what it's cracked up to be.

So that's been some themes that we've seen have emerge in the past I would say six months or so. Some other perennials are collective action. So there's a general push in terms of things that are most likely to be manipulated is anything that is likely to create collective action. That can be something for the government or against the government.

So if a nationalist calls for action -- For example, let's say there's an online conversation where the nationalists view is that China is not being tough enough on Taiwan and the nationalists call for people to go in the street, that will all be censored or there will be propaganda that's counter to that. They want to keep things down the middle of the line. They want to be in control. The CCP wants to be the one issuing the directive and not being told what policies to do.

VICE CHAIRMAN CLEVELAND: Thank you very much. It would be helpful, I think to me and perhaps other commissioners if you could come back and talk in more detail beyond today's topic, sort of what the themes are as they're emerging. Because I think your research is really important .As to whether Dr. Scissors would agree two years is longitudinal, I think we both as statisticians would say it's very short term.

MS. FAIR: Fair enough.

VICE CHAIRMAN CLEVELAND: But it's social media though, so you know -- (Simultaneous speaking.)

VICE CHAIRMAN CLEVELAND: So we've redefined -- we've redefined longitudinal. I think we're going to take a very, very brief break because I think the administration witnesses are already actually present. So if we could all be back at 1:00, which is when we're scheduled. And I apologize for that short turn around, but I also don't want to delay hearing from the administration.

Thank you, all. Kim to you, to the panelists.

COMMISSIONER GLAS: Many thanks, panelists. Thank you for your testimony.

VICE CHAIRMAN CLEVELAND: Yes. Really, really helpful. Thank you.

(Whereupon, the above-entitled matter went off the record at 12:37 p.m. and resumed at 1:04 p.m.)

ADMINISTRATIVE PANEL INTRODUCTION BY VICE CHAIRMAN ROBIN CLEVELAND, HEARING CO-CHAIR

VICE CHAIRMAN CLEVELAND: Welcome. Nice to see you. Our next panel person, we'll hear from the Department of Commerce on their progress on implementing export control reforms. Our expert here today is Jeremy Pelter, Acting Undersecretary and Deputy Undersecretary of Commerce of Industry and Security. Prior to joining BIS, Mr. Pelter served as a senior advisor to the Deputy Secretary of Commerce, advising the Deputy on issues related to policy and programming implementation. It feels like a vast universe.

Mr. Pelter entered the Career Senior Executive Service as the CFO and Director of Administration for the Economic and Statistics Administration. Before the Department of Commerce, Mr. Pelter served at the U.S. Small Business Administration in several financial and operational positions.

Mr. Pelter, you are a brave man for appearing here today. There are a lot of my colleagues who are very interested in what you have to say, as I am. So welcome and if you would proceed with your statement. Given the way we question, if you can keep it to about seven minutes, we'd appreciate it. And then you're on your own.

MR. PELTER: I appreciate your generosity and I will try to move through with the greatest haste I can.

VICE CHAIRMAN CLEVELAND: Thanks.

OPENING STATEMENT OF JEREMY PELTER, ACTING UNDERSECRETARY AND DEPUTY UNDERSECRETARY, BUREAU OF INDUSTRY AND SECURITY

MR. PELTER: Vice Chairman Cleveland and Commissioner Glas, I'd like to begin by thanking you and the Commission for the invitation to testify today regarding the export controls administered by the Bureau of Industry and Security. And to address concerns related to the People's Republic of China.

I'm honored to represent BIS today. Since my arrival at BIS in December of 2019, I've been incredibly impressed by the outstanding expert staff. As the administration has stated, the PRC poses perhaps the most complex and serious challenge to the international systems of rules and principles that reflect the values of the United States. The PRC seeks our technologies to further its military modernization through means like diverting items from civilian to military applications, creating a list of procurement networks, and stealing our intellectual property. The PRC has also engaged in human rights abuses with its campaign against Uyghurs and other minority groups in Xinjiang. We've witnessed the PRCs anti-democratic crackdown in Hong Kong. And as described in the Department of Commerce's recent report on the semiconductor supply chain, the PRC is a significant source of vulnerabilities.

All of these issues raise serious concerns. BIS is using all of the tools authorized by the Export Control Reform Act of 2014 or ECRA to protect U.S. national security and foreign policy interests that include maintaining our quality of military edge, countering the proliferation of WMDs, maintaining the health of our defense industrial base, protecting human rights, and maintaining U.S. technology leadership. I would like to take this opportunity to provide an overview of BIS's activity in this space, the role of unilateral and multilateral controls, our continuing work on emerging and foundational technologies, and the tools we are using related to the PRC.

BIS administers and enforces export controls for dual-use items, less sensitive military items, and commercial items under the Export Administration Regulations, or the EAR. BIS has additional authorities and tools to address a wide range of national security challenges. Today I will focus on export controls.

Controls administered under the EAR can be tailored to address concerns for sensitive technologies, countries entities or end uses. With respect to the PRC, we impose extensive controls including a policy of denial on applications for exports of crime control, military and spacecraft items, and generally a policy of denial for end users or use of concern, including military. All applications for the PRC are reviewed to determine the risk of diversion to a military end use or user or the potential to abuse human rights. The interagency team from the Departments of Commerce, State, Defense, and Energy that review these licenses have experts in technical policy and intelligence fields.

BIS also maintains restricted party lists like the Entity List, which currently includes about 420 Chinese entities, most of which are subject to a presumption of denial for license applications. We also maintain a Military End-User List, adding additional license requirements for 73 Chinese entities.

BIS also devotes significant resources to enforcement and is unique among agencies with its co-location of export control licensing and enforcement teams. Our enforcement authorities include criminal investigative authority for unauthorized exports, as well as investigative activities outside the United States.

The U.S. is a member for multilateral export control regimes, the Wassenaar Arrangement for conventional arms and dual use items, the Missile Technology Control Regime, and Australia Group for Chemical and Biological Weapons, and the Nuclear Suppliers Group. BIS imposes both multilateral and unilateral export controls. And it is clear that multilateral is the most effective and preferred approach as articulated in ECRAs statement of policy.

Furthermore, ECRA specifically states that export controls applied unilaterally to items widely available from foreign sources generally are less effective in preventing end users from acquiring those items. Application of unilateral export control should be limited. If BIS imposes unilateral controls and foreign suppliers exist that can backfill those orders, we will both fail to meet our goals and harm U.S. industry by creating an unfair playing field.

However, there are certainly instances in which unilateral controls are warranted. The issue of identifying emerging and foundational technologies has been raised extensively, including in a report by a commission analyst this year. We see misunderstandings about the steps BIS has taken in this effort, so I'd like to provide more on the work already done.

BIS has always worked with our partner agencies to identify new controls for emerging technologies and review existing controls on foundational technologies. Identifying these technologies will not result in the creation of a new control list. It will be cataloged and described in the existing Commerce Control List or CCL. From a government administration perspective, creating fragmented lists or indexes is never a good business practice for our stakeholders.

On emerging tech, much of the work continues with the multilateral regimes. In ECRA, Congress made clear that identifying emerging and foundational technologies should continue as a priority, in addition to the regime work. There are key factors to identifying the technology as described in ECRA.

First, identifying cutting edge developments in research requires a participation of organizations that are directly involved in funding or conducting the research often with very little historic exposure to export controls. Second, identifying emerging technologies can be particularly difficult when they are nascent or theoretical. Third, foreign availability plays a key role as required by ECRA.

For many emerging tech areas, the U.S. is only one of the countries leading in development. For foundational, the issue of foreign availability is especially challenging. The technologies already in production typically with foreign competition, making unilateral actions far less effective. Controls need careful calibration to reliably prevent PRC access and provide U.S. industry a level playing field.

BIS has taken other actions to implement ECRA like reconstituting the Emerging Technology Technical Advisory Committee with membership from academia, industry, federal labs and agencies. And we've worked with the National Security Council to organize working groups for certain technology categories. With respect to emerging technologies, BIS solicited comments from the public to identify potential emerging technologies for control under 14 categories. And for each category, an NSC working group was created to recommend new controls or review existing controls.

This work has resulted in the identification and labeling of 37 emerging technologies, all added to the CCL across fiscal years 2019, 2020, and 2021. For foundational BIS solicited public input in 2020 and has reviewed approximately 80 substantial comments. And we are preparing proposals to the relevant regimes. To address concerns related to the PRC, including its MilMod efforts and human rights abuses, we've imposed various unilateral controls.

In 2020, BIS added new license requirements for an MEU in the PRC. This control advances the objective of ECRAs foundational requirement by restricting items destined to military end users or uses, even where decontrolled at the regime level. Moreover in 2021, BIS implemented new controls that require a license for military intelligence end uses or users. BIS has also added entities to the entity list as a result of their support of China's malign activities, over two dozen in 2021 alone, either implicated in human rights abuses or for efforts in support of the PLA.

Again, the most effective controls are multilateral. But when the regimes cannot achieve our objectives, we've been working on a plurilateral basis as well. A good example is the new U.S.-EU Trade and Technology Council that includes a working group on export control. These efforts would not be complete without the ongoing work of our staff to promote compliance and conduct outreach.

Thank you again for the opportunity to testify today. I hope that this overview is helpful. And I'm happy to answer your questions.

PREPARED STATEMENT OF JEREMY PELTER, ACTING UNDERSECRETARY AND DEPUTY UNDERSECRETARY, BUREAU OF INDUSTRY AND SECURITY

UNITED STATES DEPARTMENT OF COMMERCE
Under Secretary for Industry and Security
Washington, D.C. 20230

September 8, 2021

Prepared Statement of

Jeremy Pelter
Acting Under Secretary for Industry and Security
Bureau of Industry and Security, U.S. Department of Commerce

Testimony before
the U.S.-China Economic and Security Review Commission

Hearing On
"U.S.-China Relations in 2021: Emerging Risks"

Vice Chairman Cleveland and Commissioner Glas, I would like to begin by thanking you and the rest of the Commissioners for the invitation to testify today regarding the export controls administered by the Bureau of Industry and Security (BIS) to address concerns related to the People's Republic of China (PRC).

It is my honor and pleasure to represent BIS today. The professional background and expertise I bring to BIS is most assuredly in government administration and operational management, but when the opportunity to help lead BIS arose, there is no doubt the gravity of the mission was the compelling factor in accepting this position. The complexities and challenges of that compelling mission are not lost on me. Since my arrival at BIS in December of 2019, I have relied greatly upon our outstanding, expert staff to enhance my technical knowledge and support my decision making, certainly to an incredible degree as we await the Senate confirmation of our presidentially nominated leadership. I look forward to hearing from the Commission today and the opportunity to answer some of your questions.

As President Biden has stated, democracies are in competition with autocracies in a rapidly changing 21st century, and the PRC poses perhaps the most complex and serious challenge. The PRC seeks U.S. technologies to further its military modernization, such as through diverting items from civilian to military applications (i.e., its military-civil fusion strategy), creating illicit procurement networks, and stealing intellectual property. The PRC has also been involved in human rights abuses with its campaign of repression, mass detention, and high-technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups in the Xinjiang Uyghur Autonomous Region. Additionally, the PRC has engaged in anti-democratic crackdowns in Hong Kong. In addition, as described in the Department's report on vulnerabilities in the semiconductor supply chain, issued pursuant to Executive Order 14017, the PRC is the source of significant vulnerabilities.

All of these issues raise serious concerns, and BIS has utilized all the tools authorized by the Export Control Reform Act of 2018 (ECRA) to protect United States national security and foreign policy interests. These interests include maintaining our qualitative military edge, countering proliferation of weapons and other items of concern, maintaining the health of the U.S. defense industrial base, protecting human rights, and supporting U.S. technology leadership. I would like to take the opportunity to provide an overview of BIS's activities in this space, the role of unilateral and multilateral controls, our continuing work on emerging and foundational technologies, and regulatory and enforcement tools we are using to address concerns related to the PRC.

Overview of BIS

BIS administers and enforces export controls for dual-use items, less-sensitive military items, and commercial items under the Export Administration Regulations (EAR). BIS is also one of two bureaus within the Department of Commerce that reviews foreign investments in the United States for national security concerns as part of the Committee on Foreign Investment in the United States (CFIUS). In accordance with Section 705 of the Defense Production Act of 1950 and Executive Order 13603, BIS has authority to issue mandatory surveys to key industry sectors and supply chains critical to the U.S. defense industrial base, which helps address concerns related to supply chain security. Additionally, Section 232 of the Trade Expansion Act of 1962, as amended, authorizes the Secretary of Commerce to determine the effects of imports of any articles on U.S. national security, and whether the importation of the article in question is in such quantities or under such circumstances as to threaten to impair the national security. BIS also plays a key role in industry compliance with the Chemical Weapons Convention and the Protocol Additional to the U.S. Agreement with the International Atomic Energy Agency for the Application of Safeguards within the United States. We utilize these tools to address a wide range of national security challenges, but I will focus on BIS's administration and enforcement of export controls.

The export controls administered under the EAR can be tailored to address sensitive technologies, as well as countries, entities, or end uses of concern. With respect to the PRC, BIS imposes extensive controls, including a policy of denial on license applications for exports of crime control, military, and spacecraft items. BIS also maintains a policy of denial for certain license applications involving weapons of mass destruction end uses, military end users, and military end uses. License applications for dual-use items to be exported to the PRC are generally reviewed to determine, among other things, the risk of diversion to a military end user or military end use or whether the recipient could use the items in the application to violate or abuse human rights. The officials that review these licenses are experts in their technical or policy fields, and they assist exporters in understanding the regulations, verify the proper classification of an item in the application, and determine whether the export of the items in the proposed transaction is consistent with the regulations. Additionally, all-source intelligence and investigative concerns from enforcement perspectives are factored into license decisions.

BIS also maintains various restricted party lists imposing additional license requirements or other restrictions. For example, BIS maintains the Entity List, which currently includes around 420

Chinese entities, most of which are subject to a licensing policy of presumption of denial for all items subject to BIS jurisdiction. BIS also maintains a Military End-User List, which is a non-exhaustive list of military end users that notifies exporters that a license is required for 73 Chinese entities on that list for a wide range of items subject to BIS jurisdiction.

In addition to administering these controls, BIS also devotes significant resources to enforcing them. BIS is unique among U.S. government agencies with export control responsibilities in its co-location of licensing and enforcement functions within a single agency. This structure makes information sharing more efficient and facilitates collaboration among regulators, compliance specialists, intelligence analysts, and law enforcement officers. Our enforcement authorities include searching, inspecting, detaining, and seizing items in connection with unauthorized export activity; conducting end-use checks and investigative activities outside the United States, consistent with U.S. international legal commitments and agreements – for example, by BIS Export Control Officers stationed in seven locations, including Beijing and Hong Kong; conducting criminal investigations; issuing orders denying the export privileges of those convicted of a broad range of offenses including conspiracy, smuggling, and making false statements; and imposing administrative penalties, currently rising to the greater of $311,562, or twice the value of the unauthorized transaction. In FY2020, BIS investigations related to the PRC resulted in a total of 80 months of prison time and $60,000 in criminal fines. Thus far in FY2021, BIS investigations related to the PRC have already resulted in 226 months of prison time, $1,858,000 in criminal fines, and $4,048,000 in civil penalties. BIS also has a unit that assembles, analyzes, and disseminates information from all pertinent sources to inform agencies about the *bona fides* of foreign parties for license application decisions, support designations of entities to the various restricted party lists, and to identify, impair, impede, and prevent the diversion or misuse of export-controlled items.

To further the effectiveness of our controls, BIS also conducts extensive outreach with industry, academia, and other partners to raise awareness of export control requirements and best practices for compliance. It is critical that we have an informed exporting community and that we work with them to identify potential risks. Our Office of Exporter Services provides export counselors to answer questions and organizes seminars and online tools to assist exporters. In just the first seven months of this year, we have fielded over 16,000 calls, and 4,000 emails. Moreover, we organized or participated in online seminars that attracted around 5,000 attendees and produced training videos that received almost 25,000 hits. Additionally, our Office of Export Enforcement Special Agents maintain a cooperative relationship with the exporting community; in FY2020, they conducted more than 658 enforcement outreach visits. During the same timeframe, BIS initiated 75 Project Guardian leads, which focus on apprising U.S. manufacturers and exporters of illicit procurement threats and on cooperating to identify and respond to suspicious purchase requests.

Role of Unilateral and Multilateral Controls

As part of the administration of U.S. export controls, the United States is a member of four multilateral export control regimes – the Wassenaar Arrangement (for conventional arms and dual-use items), Missile Technology Control Regime (for unmanned delivery systems), Australia Group (for items related to chemical and biological weapons), and Nuclear Suppliers Group (for

nuclear-related items). BIS works with its interagency partners to submit proposals to the four regimes and to implement the agreements reached with the other member countries.

Under the EAR, BIS imposes both multilateral and unilateral export controls, and it is clear based on our statutory authority and prior experience that multilateral controls are most effective and the preferred approach in achieving our national security and foreign policy objectives. As articulated in ECRA's Statement of Policy, Section 1752(5), "[e]xport controls should be coordinated with the multilateral export control regimes. Export controls that are multilateral are most effective, and should be tailored to focus on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States and its allies." Furthermore, Section 1752(6) of ECRA states that "[e]xport controls applied unilaterally to items widely available from foreign sources generally are less effective in preventing end-users from acquiring those items. Application of unilateral export controls should be limited for purposes of protecting specific United States national security and foreign policy interests."

We have seen these policies play out in practice. If BIS imposes unilateral controls targeting specific countries or entities and suppliers exist in other countries that can backfill orders to those targets with comparable items, then we will not achieve our national security or foreign policy objectives. The target of our unilateral action will still receive the items of concern. Also, this scenario harms our technological innovation and leadership – if U.S. companies lose sales to their competitors over time, then the loss of revenue deprives U.S. companies of the substantial revenue that funds the research and development needed to stay at the leading edge. Thus, potential unilateral controls must be carefully analyzed to assess their effectiveness on the target and impact on important U.S. industry sectors, both in the short term and long term.

To put this concern into perspective, BIS conducted studies on the impact of U.S. export controls on the space industrial base in 2007 and 2014. The U.S. space industry was studied because the United States treated commercial spacecraft items as munitions items under the International Traffic in Arms Regulations (ITAR) in 1999, whereas other countries licensed such items under their dual-use controls. The ITAR impose stricter export control requirements than the EAR, including by imposing a general license requirement for all countries and treating foreign-made items incorporating U.S.-origin ITAR content as subject to U.S. jurisdiction, regardless of the amount of such ITAR content. Thus, while most commercial spacecraft items were controlled multilaterally, the United States unilaterally treated such items as military items, which, in effect, exceeded the controls of other countries. The 2014 study (available at https://www.bis.doc.gov/index.php/documents/technology-evaluation/898-space-export-control-report/file) mentioned that the 2007 study found the U.S. share of global satellite manufacturing revenue decreased after the ITAR changes were implemented in 1999, from 63 percent in 1996-1998 to 41 percent in 2002-2005, and that lost foreign sales attributed to ITAR requirements in 2003-2006 averaged $588 million annually. The 2014 study found that survey participants "lost sales opportunities between approximately $988 million and $2 billion from 2009 to 2012." The survey participants reported various reasons for the lost sales, including giving up export opportunities to avoid the complexity of ITAR compliance requirements and foreign customers avoiding the purchasing of or designing out ITAR-related products and services. For example, one respondent stated that "customers in allied countries will do everything possible to avoid ITAR-related controls. We are the supplier of last choice."

While it's clear that multilateral controls are more effective and have fewer drawbacks than unilateral controls, there may be instances in which the U.S. Government determines that unilateral controls are warranted to address pressing and critical national security and foreign policy objectives. I will later describe both unilateral and multilateral steps we have taken as part of our unique tools to address concerns related to the PRC.

Identifying Emerging and Foundational Technologies

The issue of identifying emerging and foundational technologies has been raised extensively, including in a report issued by a Commission policy analyst earlier this year. We have found that there are misunderstandings about the steps BIS has taken in this regard, so I would like to provide greater background on this issue, the challenges we face, and the work BIS has already done.

Background

By way of background, the issue of identifying emerging and foundational technologies is not entirely new and did not originate solely with the passage of ECRA in August of 2018. BIS has always worked with its partner export control agencies to determine whether new export controls are warranted on emerging technologies and whether existing controls must be recalibrated on existing (or foundational) technologies to address new national security or foreign policy concerns. In addition, identifying emerging and foundational technologies will not result in the creation of a new list of such technologies. Such technologies will be described in BIS's existing Commerce Control List (CCL). This process follows the normal course of identifying new technology-based export controls and will also facilitate such technologies being treated as "critical technologies" for CFIUS screenings.

With respect to emerging technologies, much of this work was previously done with the four multilateral export control regimes. For example, four months before the passage of ECRA, BIS reclassified specified target assemblies and components for the production of tritium on the CCL after having previously identified the items as emerging technology and imposing temporary unilateral controls while we worked with the Nuclear Suppliers Group to impose multilateral controls. Additionally, a couple of months after the passage of ECRA, BIS implemented new controls previously agreed by the Wassenaar Arrangement on certain mask substrate blanks related to extreme ultraviolet lithography, as well as polycrystalline substrates and polycrystalline ceramic substrates. All of these technologies are now on the CCL and are controlled for export to a number of destinations, including the PRC.

With the passage of ECRA, Congress made clear that identifying emerging and foundational technologies should continue to be a key priority for the Department, in addition to traditional efforts to modernize and update the lists of controlled items under the multilateral export control regimes. ECRA mandates that the President lead an ongoing interagency effort to identify such technologies that are essential to U.S. national security. In identifying such technologies, Section 1758(a)(2)(B) of ECRA requires that the interagency effort take into account: (i) the development of emerging and foundational technologies in foreign countries, (ii) the effect

export controls imposed on emerging and foundational technologies 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.

Factors in Identifying Emerging and Foundational Technologies

There are several key factors in identifying emerging and foundational technologies meeting the criteria described in Section 1758(a)(2)(B) of ECRA. First, identifying cutting-edge developments in research requires the participation of government agencies that are directly involved in funding or conducting the research at issue. Such agencies are often not directly involved in the export control process or implementation of international trade regulations.

Second, identifying emerging technologies can be particularly difficult when such technologies are nascent or exist at a theoretical level. Under an ideal export control system, the export control agencies and the public should clearly understand the scope of controls so that they can be applied consistently and transparently. When the direction of certain research is unclear (e.g., what breakthroughs will become viable), identifying the specific technologies essential to national security – the statutory standard – is especially challenging and often requires greater time to ensure we understand the technology and potential options.

Third, foreign availability of emerging and foundational technologies plays a key role in this analysis, as required by ECRA. For many emerging technology areas, we have found that the United States is only one of many countries leading certain segments of development in the relevant technology area. In addition, there are often areas of cooperation taking place between U.S. organizations and those located in allied countries. However, we are seeing that the PRC is a near-peer competitor in many of these technology areas as well. Thus, the effectiveness of new, unilateral export controls on such technologies could be diminished in limiting the proliferation of the technology to countries of concern. Additionally, while BIS imposes new, unilateral controls when appropriate, it is possible that the imposition of such controls could hinder the development of such technologies in the United States and impact the ability for U.S. researchers to cooperate with partners in allied countries. Thus, when there is clear foreign availability, we believe that imposing new controls on emerging technologies posing national security concerns is most effective when implemented through the multilateral process.

The issue of foreign availability is the same, and likely even more pronounced, for foundational technologies. Because such technologies are already in production, there are often developers and producers of such technologies in foreign countries, thereby making new unilateral controls less effective. Additionally, foundational technology candidates can be former multilaterally controlled items that have been decontrolled, many times because of widespread foreign availability outside of regime members. As a result, we believe changes in controls for foundational technologies should be carefully calibrated, which we have done in the past for specific mature technologies that could be used by military end users or in military end uses. Further, it is important that we work with the multilateral regimes or like-minded supplier governments to review multilateral or plurilateral controls – the national security and foreign policy interests of the United States are better served if countries of concern, including the PRC,

cannot obtain the same technologies from suppliers located outside the United States. Additionally, multilateral or plurilateral controls help ensure U.S. companies compete on an even playing field with foreign competitors and are not at a competitive disadvantage, which could harm development of such technologies in the United States.

BIS Actions Taken Since the Passage of ECRA

With this background in mind, BIS has taken a number of actions to implement the objectives of ECRA. First, BIS has worked to include organizations directly involved in conducting or funding research with the review of emerging and foundational technologies. BIS convened the Emerging Technology Technical Advisory Committee after having reconstituted its membership and goals to focus on emerging and foundational technologies. Members include individuals in academia, industry, federal laboratories, and pertinent U.S. Government agencies who are engaged in the development and production of cutting-edge technologies. Also, BIS has worked with the National Security Council (NSC) to organize interagency working groups for certain technology categories. These working groups meet on a regular basis and include representatives from the Departments of Commerce, Defense, Energy, and State, as well as other agencies as warranted, such as those involved in funding or conducting the research at issue.

With respect to emerging technologies, BIS solicited comments from the public in an Advance Notice of Proposed Rulemaking on identifying potential emerging technologies warranting control, including under 14 representative technology categories. For each of these representative categories, it is possible that the NSC working group will recommend identifying emerging technologies warranting control under the criteria described in Section 1758(a)(2)(B) of ECRA. However, it is also possible that the working group will recommend that existing controls are currently sufficient for the relevant technology category or that emerging technologies in one category may overlap with those in another category.

The work with our interagency colleagues has resulted in the identification of 37 emerging technologies, all of which were added to the CCL as a result of final rules published in the *Federal Register* on May 23, 2019; January 6, 2020; June 17, 2020; and October 5, 2020. These new controls addressed some of the 14 representative technology categories as well as technologies in additional categories not previously suggested in the request for public comment. Thirty-six of these technologies were also implemented under relevant multilateral export control regimes, which both further protects such technologies from being acquired from other supplier countries and enhances U.S. national security. BIS also published a proposed control that was subsequently adopted by the relevant multilateral regime and is being finalized for publication as a final rule. In addition, BIS is working to finalize additional emerging technology proposals for review. As previously noted, this is an ongoing process.

With respect to foundational technologies, BIS solicited public input on August 27, 2020 and has reviewed approximately 80 comments. BIS is working with its interagency colleagues to submit proposals for certain foundational technologies to the relevant multilateral export control regimes. Furthermore, BIS has undertaken additional efforts, which I will discuss next, that have imposed additional controls on items subject to BIS's jurisdiction, including items that may later be identified as emerging or foundational technologies.

Given ECRA's requirement to seek multilateral controls on emerging and foundational technologies, the controls imposed to date as well as those being prepared will have specific technical parameters to facilitate adoption by the multilateral export control regimes as well as industry compliance.

Additional Tools to Address Concerns Related to the PRC

To address concerns related to the PRC, including its military modernization and human rights abuses, BIS has imposed various unilateral controls. In 2020, BIS added new license requirements for additional items subject to BIS jurisdiction if the exporter knows that the item is intended, entirely or in part, for a military end use or military end user (which includes any person or entity whose actions or functions are intended to support military end uses) in the PRC. Many of these items were multilaterally controlled but were decontrolled. This control addresses the objective of ECRA's foundational control requirement by restricting these items when destined to military end uses and end users in some of the most problematic countries that are not subject to trade embargoes.

Moreover, in 2021, BIS implemented new controls that require a license if the exporter knows that any item subject to BIS jurisdiction is intended, entirely or in part, for a military-intelligence end use or a military-intelligence end user in a certain set of countries. BIS continually assesses technologies, end uses, and end users to identify items that can be misused to engage in activities that are contrary to U.S. national security and foreign policy interests.

In addition to new controls tied to specific types of items or end users, BIS has also added entities to the Entity List as a result of their support to China's military modernization efforts and/or weapons of mass destruction programs, or their implication in human rights abuses. In 2021 alone, BIS added (i) seven Chinese supercomputing entities to the Entity List due to concerns involving these organizations' support for China's military actors, its destabilizing military modernization efforts, and/or its weapons of mass destruction programs, (ii) fourteen Chinese entities for being implicated in human rights violations and abuses in the implementation of China's campaign of repression, mass detention, and high technology surveillance against Uyghurs, Kazakhs, and other members of Muslim minority groups in the Xinjiang Uyghur Autonomous Region, and (iii) five Chinese entities for acquiring and attempting to acquire U.S. technology to support the People's Liberation Army's (PLA) military modernization, and for potential involvement in the procurement of U.S.-origin items for unauthorized military end-use. Moreover, our enforcement analysts and Special Agents continue to target illicit procurement actors who seek to obfuscate end uses and end users to circumvent export control restrictions to steal sensitive U.S. technology or acquire sensitive items, as evidenced, for example, by last month's $469,060 administrative penalty involving a U.S. company that exported semiconductor manufacturing-related items to PRC entities involved in the illicit procurement of commodities and technologies for unauthorized military end-use in China.

As I mentioned previously, however, the most effective controls are those that are multilateral. To that end, we are working through the multilateral regimes to propose and implement new

controls on certain items. Additionally, as discussed above, when the multilateral regimes cannot achieve our objectives, we are working on a plurilateral basis with likeminded countries. We are also working to coordinate on those items that are already controlled. For example, the United States and European Union have established the U.S.-EU Trade and Technology Council, which will include a working group on export controls. We are also continuing bilateral discussions with allied countries, especially those supplier countries of certain technologies of concern, to coordinate on common controls and policies. Specifically, we are working to share information and reach an understanding with our allies on coordinating license review policy for various types of technologies and seek to have them take into account our restricted party lists when evaluating whether to approve a license. Our engagement with allies is critical to the long-term success of our efforts to address national security and foreign policy concerns related to the PRC.

These efforts would not be complete without the continued work of our staff to promote compliance with our controls related to the PRC and conduct outreach with the exporting community. In July of this year, BIS hosted its first China Academia Conference to discuss threats posed by certain elements of PRC-linked academia. The briefings were delivered by U.S. and other Western academics to give the audience a unique perspective on issues and potential actions. The conference was attended by over 200 individuals from 18 government organizations and 38 academic institutions. BIS is leveraging these unique relationships to develop new tools to assist universities comply with the EAR and identify attempts to misappropriate U.S. intellectual property to prevent its export and identify enforcement leads to disrupt and deter these illicit activities.

Finally, just last week, BIS hosted its annual Update Conference, which attracted hundreds of participants to the virtual event. The conference featured representatives from BIS our interagency colleagues to discuss a number of export control topics, including controls related to military end users and military end uses in China as well as foreign policy-based controls addressing human rights and other concerns. BIS continues to be engaged with the exporting community to keep them informed on our controls.

Conclusion

Thank you again for the opportunity to testify. I hope that this overview of BIS's administration and enforcement of export controls is helpful to the Commission's review of emerging risks related to U.S.-China relations. BIS will continue to work with our interagency partners, Congress, the exporting community, and counterparts in allied countries to further our national security and foreign policy objectives. I am now happy to answer your questions.

VICE CHAIRMAN CLEVELAND: We'll interpret that "happy" loosely. Is Chairman Bartholomew there? If not, I'll turn to --

CHAIRMAN BARTHOLOMEW: Yes, I am. Thank you. Secretary Pelter, thank you very much for appearing today before us. I wanted to express appreciation to you and to all of the staff at BIS for all of the work that you do to meet these goals.

I guess what really hits me is does the technological innovation and bureaucracy really work at different paces? So I wondered if there are things that Congress could do to help BIS meet the goals that we all share?

MR. PELTER: Thank you for the question, Commissioner. You're absolutely right. The pace of government and government regulation does not move as quickly as we see the speed of technology move. I think when it comes to how Congress can support the Executive Branch in continuing our efforts, it's through consistent collaboration and engagement in a productive manner to ensure that the resources are in the right places, the appropriate departments, agencies are working together. And the recommendations that come through those processes are looked at, understood, and implemented as possible.

CHAIRMAN BARTHOLOMEW: So to put you on the spot, is there anything specifically that you can mention in terms of what needs to be done to get agencies -- to other agencies to work with you or to facilitate things taking place?

MR. PELTER: I think we have an outstanding relationship with our interagency that for the most part includes the Departments of State, Defense, and Energy. That interagency process works exceptionally well. The NSC is a great coordinating party as well. So I don't know that there's something necessarily we would look to Congress to support in that area, but we are always open to continuing the conversations. And if the Commission has ideas in that space, we'd be open to working with you as well.

CHAIRMAN BARTHOLOMEW: Alright, thank you. I will yield back the balance of my time.

VICE CHAIRMAN CLEVELAND: Thank you. I'm going to yield my time to Commissioner Scissors for the moment. Well sorry about that. The staff gave me a list that says Bartholomew, Cleveland, Borochoff because I guess -- and I just follow instructions -- but go for it.

COMMISSIONER BOROCHOFF: I remember the time that I thought you weren't in the room and you were sitting next to me. So I guess we're now even.

VICE CHAIRMAN CLEVELAND: Sorry about that.

COMMISSIONER BOROCHOFF: No, no problem. I'm a business person owner for over 40 years. And so I really truly appreciate everything that you've said and I do honestly believe that the Government and particularly your department has a broad portfolio that makes it incredibly difficult to move the ball down the field. But I was going to ask almost the same question that Chairman Bartholomew did. And I think what I heard you say to us was, you know, hey we're open to suggestion.

And in my business when we have experts in the business, I can't usually give them the suggestions. I want them to give me the suggestions so we can evaluate it. So I'm going to ask it slightly different, but it's almost entirely the same question so please forgive me. If you were in charge of all the sister agencies that you deal with, if you were in charge of the Executive Branch and you had your own wish list, what would you change to speed things up?

Because what I've been hearing for quite some time and when I read the literature about the entity lists and the technology speed, I agree with what you said. There's no question about it. But there's a strong desire in our country and amongst businesses and government for you all to be able to move a little more quickly. What would you do to make that happen?

MR. PELTER: Well if I was in charge of everything, it would be very easy. I would just tell everybody what I wanted them to do and we'd get it completed.

COMMISSIONER BOROCHOFF: I'd accept that.

MR. PELTER: I think I would look at it from maybe two directions. The first probably being very colored by our experience during the COVID-19 pandemic. You can never have too much information and communication among agencies. And while we do a fantastic job with that, we also need to work to ensure that our datasets, our information whether it's at the Department of Commerce or Defense, Energy, State, wherever it may be is shared. And shared in the fullest and speediest way possible.

One thing we've noticed is that with the pandemic, you know, an awful lot of business gets done kind of in the side conversations, in the hallway meetings. You know, particularly in those face to face environments. And that's something that's been a challenge right now. It's a lot easier to work out your differences when you're sitting across the table and you can have small group or one on one conversations. And so that's a difficult thing to legislate.

So we'll hope that our continued efforts to get this pandemic behind us pay off. But I think what that tells me too is that we need to find more novel and unique ways to get our folks connected all the way up from the staff level to the Assistant Secretary level and above. And make sure those conversations are happening in a meaningful way.

On the other side of it, again sharing those data sets and ensuring that there are no barriers to those sets of information moving from agency to agency, whether it's a statutory barrier, a regulatory barrier, or many times we find in the federal government, an information technology barrier. So those would be the things that I would think about that would help improve the pace with which we can try to keep up with technology.

COMMISSIONER BOROCHOFF: So I'm going to follow up with a really quick one.

MR. PELTER: Sure.

COMMISSIONER BOROCHOFF: Those were two really good concrete answers and I thank you for that. So are you saying then that before the pandemic, the cooperation was way better and things happened more quickly?

MR. PELTER: I wouldn't say the cooperation was better. I think the relationships we have among the interagency are outstanding. They are cooperative. They're adversarial when they need to be adversarial. We certainly don't want to keep opinions off the table in the name of getting along. But I think what's been lost is some of those small group and light conversations that kind of help advance the ideas. And it is just different when you're on MS Teams call or a conference call and you're not seeing people face to face to getting across on some of those nuts and bolts that sometimes can hold us up.

COMMISSIONER BOROCHOFF: Thanks for that answer.

VICE CHAIRMAN CLEVELAND: I'm going to use your 51 seconds before I yield all my time to Commissioner Scissors. In my experience on the NSC and CFIUS, there was never an occasion when we met where any agency that wanted to participate could participate, whether deputized as the lead or not. In your experience, has there ever been an agency who has been excluded from participation in a CFIUS decision?

MR. PELTER: I'm not aware of any instance in my firsthand experience where an agency has requested to be engaged in a CFIUS transaction review and been denied that opportunity. Generally we look for a big tent when it comes to CFIUS transactions or other interagency processes.

VICE CHAIRMAN CLEVELAND: Okay. If we reset the clock for my time and I am yielding my time to Commissioner Dr. Scissors.

COMMISSIONER SCISSORS: Thank you, Vice Chair Commissioner Cleveland. Under Secretary Pelter, from your written testimony -- this is a quote -- "with the passage of ECRA, Congress made clear that identifying emerging and foundational technologies should continue to be a key priority for the Department". I believe you said something very similar just now in your oral testimony.

Congress did not pass ECRA for BIS to continue to prioritize these technologies as it had. Congress found existing identification of emerging and foundational technologies among other things to be inadequate. That statement is the background music for many questions I have -- Thank you, Commissioner Cleveland -- which we probably won't get all of them -- to all of them.

The first set, you also said -- again, this is a quote from your written testimony. BIS will follow "the normal course of identifying new technology-based export controls." So first set of questions, the normal course as of when? Do you think Congress passed ECRA so that BIS could continue to follow its normal course of identification as of pre-ECRA? If not, then BIS created a new course post-ECRA. Great. What is the biggest point of departure in the new course from the previous course?

MR. PELTER: So first, I'm grateful and it happened before my arrival at BIS, but I'm grateful for the passage of ECRA. Having that permanent statutory authority is a significant step from the executive order extensions of the EAA. I think it brings both stability to our programs, as well as the enforcement activities and all the activities we do at BIS.

When I look at the language in ECRA -- and I am certainly open-minded. I am also not a statutory scholar, so I won't present myself to be one. But when I look at the language, it pushes us to do two things. Keep emerging and foundational technology at the forefront of our activities. And two, start to look at nontraditional avenues for identifying emerging and foundational technologies and get processes into place to try to attack that issue.

When I think of the, you know, normal or traditional ways in which these technologies were identified, the CFIUS process comes to mind. The license application process comes to mind. Commodity jurisdiction requests come to mind, commodity classification requests come to mind. And then the interagency licensing process itself.

When we think about nontraditional methods, what we're looking and trying to do and have been doing with some very good success is engaging a much broader set of stakeholders into our process. We have a much more significant engagement with academia. We just recently had a China-based academia conference trying to identify and better understand how we can prevent PLA-backed Chinese academia from getting their hands on sensitive technologies. There was over 200 representatives across industries, federal labs, academia, and elsewhere. So those are the types of -- some of the types of activities we're doing.

We've reestablished the Emerging Technology TAC. That was an important step. It's got a very broad membership. That membership again includes folks from industry, academia, other federal agencies. You know, we're always looking for a big tent. And if folks that are interested in being engaged in that technical advisory committee get engaged with us, we make it happen.

I think the other thing we've been doing again is this set of NSC working groups. We looked at the categories of emerging technology that we felt were the broad based sets ready for review, put that out for public comment. Took the public comment put together with the coordination of the NSC, these working groups. And they're working hard through that process. And so I think these are kind of the nontraditional, new processes and routines that we've put in place to try to deal with the issue.

COMMISSIONER SCISSORS: Thanks for your answer. I want to pick up on those 14 working groups. I know that BIS doesn't like the idea of a list, but there are actually two lists. There's the 14 technologies group list and there's the 37 you've added to the CCL list. I understand the objection that hey, we may not take action in all 14 of those technologies. You said that in your written testimony. That seems fine. I understand that you're saying hey, don't -- thirty-seven isn't everything. We're not done. I get that too.

But I think Congress would find that inaction say 11 of the 14 technology groups would be a bit dubious. That hasn't happened. I was just giving an example. I don't know how to relate 37 to the universe. So I have a question based on in fact two lists of sorts that BIS has created that we're being warned off of using as formal lists. What metric should Congress use to judge BIS's progress on emerging technologies?

I mean you know, three years have passed. You have a couple of lists. Is it 37, but we should have had 70 by now? Is it we're going to work on 14 and we've only made progress on two? If we're not supposed to use things BIS has said and say okay, well this is the standard by which we can judge because the process is ongoing, how is BIS to be judged on emerging technologies?

MR. PELTER: That's a great question, Commissioner. Thank you for asking. When I look at it, I think of it in a couple of ways. So first of all, we know there will never be an exhaustive list of emerging technologies. By definition, they continue to emerge. We continue to need to review them and we continue to need to control them. If there's a belief that our pace has not been fast enough, that we need to put our foot harder down on the gas, I think that's constructive criticism I'm willing to take back. I'll talk with our team. Talk with our stakeholders here on the Hill, this Commission, Congress, committees and work through that process.

I don't think that there is a specific quantitative answer to how many technologies should be controlled? At what pace and to what volume of controls there should be. I like to look at it from a qualitative perspective of when we can identify an emerging technology. When we can diagnose what the risk is to our national security, our foreign policy interest, and we can back that with facts and analysis. Then we take action and we get the support of our interagency partners to do that.

COMMISSIONER SCISSORS: Thank you. I am out of time, at least my initial time.

VICE CHAIRMAN CLEVELAND: Commissioner Fiedler, yes, are you online?

COMMISSIONER FIEDLER: Can you hear me?

VICE CHAIRMAN CLEVELAND: Yes, we can.

COMMISSIONER FIEDLER: So investment in new and foundational technologies is largely the purview of private equity. And Chinese military companies have their own investment farms. Has BIS identified them?

MR. PELTER: Thank you, Commissioner. We've put an awful lot of time in research. We have an outstanding Office of Enforcement Analysis, as well as our Export Enforcement

Team that look at these issues. We also leverage the minds and intelligence of our interagency partners; again including -- and most particular, I think to your question, the Department of State and the Department of Defense. So we do look at these.

Many of these institutes -- PLA-backed institutes or research companies have been placed on our Entity List or labeled as military end users. This is also a place where the Military End-Use Rule specifically helps prevent technology from reaching those research institutions that are linked to the PLA. So I think we've done good work in this space. Again, that is another area where we will likely always be chasing new entities and we will never be able to have an exhaustive list. But I can guarantee our energy won't be exhausted in this space either.

COMMISSIONER FIEDLER: Following up on -- How is your ability to track U.S. private equity investments in what you've deemed internally troublesome PRC companies that are working with foundational or new technology?

MR. PELTER: So I think the Ambassador Tai, a U.S. trade representative has been out front that there's a China policy review underway. I certainly wouldn't want to get out ahead of that review. But I do know and it's been publically reported that there's a significant look happening on outbound investment into China and the risks that poses, both between U.S. capital potentially providing infusions to adversarial entities, as well as the concern over tech transfer or even coerced tech transfers as part of those investments. So it's something we're looking at. I know that there's a U.S. government working group. And certainly we will continue to add our voice to any of those opportunities.

COMMISSIONER FIEDLER: Do you view your sources of information on U.S. private equity investments as exhaustive enough?

MR. PELTER: I think we rely on a lot of open source information. I think we rely significantly in this space on our interagency partners. This would also be somewhere I'd probably defer to the Department of Treasury and other federal agencies for kind of the fullness or completeness of the information that we have available.

COMMISSIONER FIEDLER: So you're shoving the responsibility off on their other agencies? So who is responsible for tracking U.S. private equity investments in Chinese companies?

MR. PELTER: Well I certainly don't want to pass the buck. I think it's a whole of government issue and a whole of government effort. I would certainly say when we're looking at foreign investment leaving the United States, I would think the Treasury Department is probably the key leader in that area.

COMMISSIONER FIEDLER: So they provide you information when you ask for it?

MR. PELTER: I'm not aware of any instance where we've been working with the Treasury Department or any other federal agency to get information and we've been denied. Certainly as I mentioned before, information sharing sometimes could be sped up.

COMMISSIONER FIEDLER: How often do they say that we don't know?

MR. PELTER: I'm not aware of any instance where we've simply gotten a "we don't have anything" response. But I can certainly go back to my team and ask them for more information and follow up with the Commission.

VICE CHAIRMAN CLEVELAND: Jeff, I'm not sure we heard you if you --

COMMISSIONER FIEDLER: I'm done.

VICE CHAIRMAN CLEVELAND: Oh, okay.

COMMISSIONER FIEDLER: I'm finished.

VICE CHAIRMAN CLEVELAND: Well, heard you. Commissioner Glas.

COMMISSIONER GLAS: Thank you, Undersecretary, for coming to testify today. I'm going to defer my time to Commissioner Wessel.

COMMISSIONER WESSEL: Thank you, Madam Co-Chair. And thank you, Mr. Secretary for appearing today. And I know that there was some concern about a staff report that was issued by the Commission. I have to say that your comments that, that question -- that study questioned the expertise and diligence of your staff is certainly not the object. I don't believe that it did. And in fact, I stand by what our staff has done. I think they've done exceptional work. I think what our study questioned was the implementation and the policy decisions that appear to have been made or are being made.

I've been doing this a long time, 40 years. I was Staff Director for the House leadership for Exon-Florio in the '88 Act. And I was part of a small working group with Heath Tarbert and others, Derek was part of it -- regarding some of the reforms that were done.

And the congressional intent was that the list for foundational and critical technologies would help guide the public markets. It would guide investors, would guide companies, give them more certainty. And my fear is that the slow process appears to potentially be a policy decision, that rather than to speed up and address the emerging technologies as they are being brought to market that we have substituted a multilateral focus which is exceptionally slow, which from a policies perspective diminishes the energy and activism that started with the last administration.

And so from a policy basis, are your comments with your testimony today, comments about the staff report, et cetera, a sign that BIS thinks we have been going too quickly and need to pull the reins in significantly?

MR. PELTER: Commissioner, let make just make sure I understand. When you say we've been going too swiftly and need to pull the reigns in, you're referring specifically to the identification of emerging and foundational technologies?

COMMISSIONER WESSEL: It's the -- correct, the entity listing, et cetera. But now, understanding there was a lot of criticism of the Trump administration for unilateralism versus engaging our multilateral allies, we saw it, as you know, in 5G and many other areas.

While it appears that multilateralism, as you've described, really should be the number one goal. For certainty or benefits to the market, you point out that going unilaterally puts at risk U.S. companies who may be closed out of a market.

But for those of us who were involved in the drafting and from Congressional, you know, review -- not review -- Congressional input at the time, they wanted BIS to be keeping pace with emerging technologies and driving results rather than responding to them on slower term.

MR. PELTER: All right, thank you, Commissioner. I certainly won't try to match your historical perspective in how the legislation was drafted.

I think I will comment on a couple of points you made. One, there's absolutely no policy for BIS to move slow when it comes to identifying emerging and foundational technologies.

I'm receptive to constructive criticism if folks think that we do need to step on the gas pedal harder. We can look if there's -- look and see if there's ways to do that. I'm happy to work with my team, the Commission and other stakeholders to think about ways to do that.

But as I said, over the last three fiscal years, we've labeled 37 emerging technologies. We want to keep the pace moving, but we need to do it with great care.

When there's exigent national security circumstances or if we have strategic control over a choke-point technology, unilateral actions regarding a control of a technology or a broad set of technologies can be very effective.

When there's significant foreign availability, we are setting ourselves up for a rule that could have unreliable effectiveness and could simply punish U.S. businesses while foreign businesses are boosted in the exact same field, and the PRC gets its hands on the exact same technologies.

I think what I'd like to express is that we plan to continue moving forward with multilateral controls through the regimes. Where those aren't available, we're going to achieve our goals, work in a plurilateral way with a small set of partners, specifically when there's a small set of partners that may control a strategic choke-point technology and then use, as needed, unilateral controls.

We use unilateral controls not on specific technologies, but very much on specific entities that we don't want to access to sensitive technologies as well as larger sectors, just as we did with the MEU.

Again, open to continued conversations on our pace, open to thoughts on what might help improve our pace. But any time we're controlling business through regulation, we need to do it with great care.

And we need to ensure that there aren't unintended long-term negative consequences to what we're doing. Thank you, sir.

COMMISSIONER WESSEL: Thank you. Madam Chair, since I had time ceded to me, if I can use my later time as well, just to follow up here. And thank you, Mr. Secretary, for that comment.

As you know, this is all going to come to a head probably in the next several months as the permanent nominee is going to be considered by the Senate, whenever that process occurs. And this really -- BIS, in my view, is probably the sister act, if you will, for USTR in terms of trade policy and how we address the China challenge.

And I appreciate your offer to work with us on how to speed things up. We certainly stand -- I certainly stand ready to do it and I'm sure my colleagues do as well.

But I think the question about, you know, both the multilateral system as well as the question of not adversely impacting U.S. business doesn't do justice to the question about deemed exports, the question that you raised or the point you raised earlier about work with universities and colleges.

The fact is that I think most people -- I certainly view the U.S. as still the great innovator of technology. And for many of those technologies, they've been slipping out of our hands to China, both through licit and illicit means.

So the work that your department, your group does -- great people -- is really key to whether we are going to be able to retain and reclaim our technological leap.
How are you going to integrate all of this? How do deemed exports work within your view on the lists? And how are we going to run faster to keep leadership?

MR. PELTER: Thank you for the question, Commissioner. And first, let me share that I absolutely feel the gravity of the mission of the Bureau of Industry and Security. And I appreciate your comments, elevating us to such a degree in the importance of what we do.

Deemed exports is certainly a challenge. We live in an information age when information can be very easily displayed to those that may not have our best interests at heart.

We also live in an information age where it is very difficult to keep electrons from moving across oceans and from one country to another. And so it's a significant issue.

I think what we do that's most important is putting our energy in and prioritizing our energy into controlling the most sensitive technologies to the most sensitive destinations for the most sensitive end uses.

And while we do that, putting controls in place, we feel that continue to support that mission of protection. It is a real challenge. In deemed exports, information sharing, the digital world can be an extreme challenge.

But it's something that we have to continue to think about and continue to try to combat, particularly when we're talking about, as I said, the most sensitive technologies, things that can be supportive of weapons of mass destruction proliferation, chemical weapon precursors, even leading-edge semiconductor technology.

COMMISSIONER WESSEL: All right, thank you for that. Let me ask also, for end user verifications, since again it's not only the pace at which we control things but for those items that -- licenses, et cetera -- have been granted to.

My understanding is the ability to do those end user verifications has been severely constrained during this period of COVID. Can you provide any information on that and how, if at all, we can improve in that area?

MR. PELTER: So we have an outstanding team of export control officers that are placed strategically, internationally. And they do an outstanding job in their work.

One of the key components of that is end use checks. In most cases physically going out to locations to look at technologies that's been licensed for export and delivered, ensure that the technology is there and that it's being used for the purpose that was stated in the license that was approved. Absolutely, COVID has posed a challenge there. I don't think there would be anybody worldwide that would say travel during the pandemic has just been business as usual.
So that has absolutely been a challenge. We've worked through that in a variety of ways including virtual checks where possible and then travel even under difficult conditions where possible.

I do hope, as I said before, that soon this pandemic will be behind us and we'll be able to go back to the standard operation procedure for end use checks that both takes into consideration the national security concerns we have in that program, a couple of the health and safety of our staff members that do that important work.

COMMISSIONER WESSEL: And thank you for that and, you know, certainly the health and safety of our personnel is, you know, of paramount concern.
If travel restrictions continue, is there some plan to potentially slow the pace of licenses so that we have adequate end user verifications to secure America's interests?

MR. PELTER: I've not had any discussions about an intentional policy to slow the pace of licenses. I think we could look at very specific entities where we've not been able to perform an end use check of potentially the most sensitive items and if needed, take a look at what licenses are outstanding and ensure that the interagency team of Commerce, Defense, State and Energy are still comfortable with the licenses approval prior to an end use check being conducted.

COMMISSIONER WESSEL: All right, thank you. And thank you for appearing today and for your team's work.

VICE CHAIRMAN CLEVELAND: Commissioner Kamphausen?

COMMISSIONER KAMPHAUSEN: I'm going to yield my time to Commissioner Scissors, and thank you, Secretary Pelter, for coming today.

VICE CHAIRMAN CLEVELAND: So that means, Commissioner Scissors, you have Mr. Kamphausen's time and your time.

COMMISSIONER SCISSORS: Oh, this is going to be so fun.

VICE CHAIRMAN CLEVELAND: And then Senator Talent, you'll follow.

COMMISSIONER SCISSORS: I have another metric question. On emerging metric for judging BIS's progress, I get the arguments on emerging technologies that they're emerging. So, of course, it's ongoing. And also, it's hard to tell what the threat level of the technology is when it first exists and who has it.

And that would be a reason for why maybe members of Congress were -- me or other members of the Commission or others might want some dramatic action on emerging technology is impossible.

Those comments do not, however, apply to foundational technology. And in particular, it took two years for the first notice with regard to foundational technology to be issued. Those technologies are clear. The first notice is not the final rule. We're not making U.S. policy without consideration. There's no excuse, in my mind, for that whatsoever.

It's been another year now, over a year, and nothing has been done as a follow-up. I'm going to try to preempt your answer. If I'm wrong about your answer, then tell me I'm wrong. That would be great.

But the answer that I've had in discussions with BIS officials in the past is, well, foundational technologies involve -- obviously, they more involve multilateral controls because they're more widespread available technology.

So my metric question is, first of all, in my opinion, BIS has already messed up because it should have started this process very quickly, knowing what the technologies were. It couldn't go as -- it couldn't finish the process, but they should have been started earlier. But how many years should Congress, having passed ECRA, wait for action on foundational technology for the sake of BIS finding the multilateral system sufficiently accommodating? In other words, you said correctly, in your testimony, and others have as well, there's a tradeoff here between speed and comprehensiveness.

Well, it's been three years and we've done almost nothing. Are we looking at three more years for action on foundational technology as mandated by ECRA? Two years? What's the metric here?

MR. PELTER: Thank you, Commissioner. And I appreciate you highlighting the challenges here. And certainly some of my answer that you projected are absolutely part of my answer.

I will not back down from the idea that I think controlling these technologies through the multilateral regimes is the best way to do it. If we're not successful there, we should be looking at plurilateral scenarios that will help prevent the PRC from getting the technology. If it's widely available and we're simply doing a unilateral control, the PRC will get the technology from elsewhere, our industry will be harmed and we will have gained nothing. Foreign availability is particularly clear here. And when we're talking about foundational technology, as you said, sir, we are looking at technologies that have been around and are available.

And in fact, some of these technologies were previously controlled multilaterally and then decontrolled because of the wide availability.

When I look at what BIS had done already in this space, I have to point to some of the actions that we've taken, most particularly with the entity list and rules like the MEU.
We are trying to take a targeted approach to prevent the countries of most concern as well as the entities of most concern from getting their hands on this technology and being approved for licenses.

As we look at foundational technology and we look at what warrants control, we are working very closely with our interagency partners at the Department of State, Defense, and Energy.

I take your criticism to heart. I think it's important that we continue to move forward in this space. I do think the multilateral approach I best.

If there's a foundational technology where we control -- it is a strategic choke-point, I think that's a different scenario. And I'll continue to work with my team to advance the ball here and continue to work with the Commission and our Congressional stakeholders and others on their expectations of the Bureau.

COMMISSIONER SCISSORS: So, let just ask a quick follow-up on that to clarify. You are -- I'm not talking about a comprehensive set of foundational technologies. I'm asking when there would be an action along the -- you know, it could be a small action, right. We had -- the emerging technologies are not done. Nobody said they were.

Any action -- when's the timeframe for an action by BIS on foundational technologies? Incorporating -- we may have different views on how important multilateral cooperation is.
But incorporating your view, is it a year? Is it two years? Do you have any sense of that?

MR. PELTER: Sir, I'm going to refrain from putting a timeline on, you know, where we are in the process here. And I will also refrain from discussing any specific deliberations we're having.

But I can tell you that we are working on it. It is on my radar. It is a blinking, bright light on my radar. And we are working to get there.

COMMISSIONER SCISSORS: All right, let me ask a question on the Entity List and other authorities that you just mentioned.

The Entity List, of course, merely requires a license. It's not a prohibition. I'm not blaming BIS for that. You know, Congress has the opportunity to prohibit exports. It's used as a licensing process.

But I am curious, have you, while in your time at BIS, made available to Congress aggregate figures -- not identifying companies, of course -- on a number of licenses applied for, rejected and accepted?

In other words, I get questions from staffers and members of Congress saying, you know, oh, there was a story about so-and-so getting a license. Well, that's one. What they're really looking for is large numbers. Have you made available to the Congress a time series, say, of, we got this many applications in 2019, this many in 2020; this many were accepted, this many were rejected?

MR. PELTER: So, Commissioner, thank you for the question. The general answer is yes.

COMMISSIONER SCISSORS: Okay.

MR. PELTER: Under ECRA in 1761(h) -- hopefully, I got the citation right -- BIS has a duty of care to keep licensing information confidential.

However, information can be shared by the relevant committees, the appropriate committees of jurisdiction.

And we typically work that process through a letter on committee letterhead from the committee chairman or the ranking member.

I'm not aware of any instance where, within the bounds of what we're able to provide through that section, that we've not provided it.

COMMISSIONER SCISSORS: Thank you. Somewhat related, the Foreign Direct Product Rule has been used to enhance restrictions on Huawei but not, as far as I know, Hikvision and other actors which benefit from American technology and act contrary to our national interests.

Please correct me if I'm wrong, but the application seems very narrow. I would like to know why. There may be reasons for it to be narrow.

I'm a little suspicious of it only being applied to Huawei because, as you know very well, Huawei has become this political touchstone. So if I'm wrong about application to Foreign Direct -- and I don't blame BIS for that. If I can shoot myself in the foot, I blame Congress. You can strike that from the record, whoever is doing this. If the Foreign Direct Product Rule has been applied more broadly, please correct me. If it has been applied quite narrowly, could you explain why that's the case?

MR. PELTER: Thank you, Commissioner. And we've had a lot of questions on the Foreign Direct Product Rule. It certainly is a hot topic and you're absolutely right, its application to Huawei is a hot topic as well.

I think the Foreign Direct Product Rule can be a very powerful tool. And we've seen that in its application with Huawei, preventing them from using U.S. technology to advance malign behaviors.

Like any tool, particularly a powerful tool, it needs to be used judiciously and will be most effective where significant choke-point technologies are involved and they're of U.S. origin.

If it's used injudiciously, there is certainly a risk of unnecessary negative consequences to industry and not just use in China but also by our international partners.

And again, you and I have repeated my phrases. You know, I still believe multilateral controls are the most effective and best tools. The FDPR is certainly an available alternative tool.

I'll refrain from comment on any existing deliberations among the interagency pertaining to the FDPR. But, like all of our regulations, we work through a process with our interagency partners. That includes not only the NSC but State, Energy and Defense.

COMMISSIONER SCISSORS: Okay, my last question, to the relief of everyone in the room except me, your written testimony shows a surge in BIS enforcement actions in fiscal '21 over fiscal year '20. So I can ask this in two different ways. Why was there so little enforcement in fiscal year '20? Or why is there so much enforcement in '21? Did criminal activity rise? You know, what's the explanation? And there may be a very -- a wonderful, assuring explanation, but I'd like to know where the jump comes from.

MR. PELTER: I'm going to be very honest with you, sir, and I don't have a concrete answer for that today. But I'd be happy to work with my team and follow up with you on that.

COMMISSIONER SCISSORS: Okay.

MR. PELTER: That's not necessarily a question I had anticipated. I do know that 2021 has already been started off as a banner year.

I believe we've got about 226 months of prison time that have been handed out; $1.9 million in criminal penalties and I think just over $4 million in administrative penalties. So it has been a good year for enforcement.

I guess a year that required zero enforcement might be the best outcome for the United States government and the taxpayer, but the Office of Export Enforcement team is working very hard and they're chasing down every lead. The difference between '20 and '21 I'll have to get back to you on.

COMMISSIONER SCISSORS: I will -- I'll have it submitted as a question for the record. Thank you.

MR. PELTER: Terrific. We'll be happy to respond.

COMMISSIONER SCISSORS: I yield back my last two seconds.

VICE CHAIRMAN CLEVELAND: I think we've run over already. And I certainly appreciate the indulgence of Mr. Pelter. I'm hoping that you'll stay for a few more minutes --

MR. PELTER: Yes, ma'am.

VICE CHAIRMAN CLEVELAND: -- and allow Senator Talent and --

COMMISSIONER TALENT: I just have one question -- who?

VICE CHAIRMAN CLEVELAND: -- Commissioner Wong to -- both of you.

COMMISSIONER TALENT: Okay, because you've mentioned the importance of acting multilaterally and you're working very hard to do that.

So how would you sum up the reception of the attitude of our partners or potential partners in this? Are they getting more cooperative, less so?

I don't expect you to go into specifics here, but -- I mean, are you achieving some success in getting them to support you in this?

MR. PELTER: I believe so, sir. I think we've seen very promising collaboration from several key partners in Asia and in Europe. I will also add a great example of where this process is advancing is the new EU U.S. Trade and Technology Council that's standing up with a Working Group for Export Controls.

That is an incredible amount of cooperation. I think we're going to continue to see our allies, our like-minded trade partners and others, come to the same realizations about the PRC and their maligned activities that the United States has seen for many years.

I think that education campaign, that collaboration campaign, that coordination campaign is working well. I think the relationships are sound. And we're excited to be working with partners internationally to get the most effective controls in place.

COMMISSIONER TALENT: Thank you. Thank you for coming. It's been very informative and helpful. Good to hear your point of view.

Not every administration, every time, has been willing to send people down here. We understand that, but I'm grateful you're here.

MR. PELTER: Thank you, sir.

VICE CHAIRMAN CLEVELAND: Thank you. And, Commissioner Wong?

COMMISSIONER WONG: Mr. Secretary, thanks for coming. I echo Senator Talent and everyone's thanks for you coming down and sharing your opinion.

Mine is just kind of a small question, more of a curiosity than anything. In identifying -- we're in the process of identifying emerging technologies, foundational technologies -- you talked about interagency process.

I assume, but maybe I'm wrong, that a large part of that process is that you consider the technologies that China itself has either announced publicly or that we know that they are pursuing, you know, from other OCENT (phonetic) or clandestine collecting that we're just looking at what they want and what they're trying to pursue. Is that right?

MR. PELTER: So that's certainly a piece of it. And we absolutely use Open Source and other source information to help us in this process.

And I think a lot of the work we've been doing is making a difference. And we can see this in some of China's outrageous rhetoric out there in the public space where they're trying to invest their dollars.

We saw -- just today, I saw -- maybe it popped up last night -- a new report that the Shanghai government is going to be supporting a $9 billion investment into SMIC's Legacy chips fabrication efforts.

These are the types of reports that help us -- help inform us about, you know, where they're targeting and what they're looking for. We use other sources of information as well, but we absolutely want to be informed.

We want to make sure our energy -- that we're burning our calories on the technologies that are most critical, that the PRC is moving after most aggressively and particularly the spaces where we have still -- whether it's U.S. technology alone or U.S. technology in concert with like-minded nations and allies where we still have a significant leading edge and that the PRC is not a near peer of ours.

These are the places where I think we can have the most impact. And so we -- just like we want to be a big tent when it comes to people that can give us good credible information, we want to be a big tent when it comes to all sources of information to help inform our rule-making.

COMMISSIONER WONG: When we have that information, and in our discussions in the multilateral setting or the plurilateral setting, do we share most of that or all that information about Chinese intentions and actions to collect on -- or pursue these technologies?

MR. PELTER: There's certainly no restriction on sharing Open Source information, media reporting, PRC public announcements about what they're working on or where they're investing. If it comes to other source information, it would certainly be dictated by the specifics of the information.

COMMISSIONER WONG: Thank you.

VICE CHAIRMAN CLEVELAND: Thank you very much. We appreciate your appearing and answering questions. And I think it has been helpful to get your perspective. There probably will be questions for the record.

Given the timing of our report, I would hope that you could be quick in the turnaround so that we can make sure to incorporate your perspective. I think what we'll do is take a very brief thank you -- take a very, very brief 5-minute break and then turn to the next panel because we were supposed to start at 1:00. And so if members could excuse or come back as needed, but, Kim, I'll turn it over to you to start again in five minutes. Does that work?

COMMISSIONER GLAS: That works. Thank you.

VICE CHAIRMAN CLEVELAND: Okay. All right, thanks.

(Whereupon, the above-entitled matter went off the record at 2:01 p.m. and resumed at 2:06 p.m.)

PANEL III INTRODUCTION BY COMMISSIONER KIMBERLY T. GLAS

COMMISSIONER GLAS: Thank you so much. For our next panel, we will discuss the status of U.S. Export Controls and Investment Screening.

First, we welcome back Kevin Wolf, partner at Akin Gump. Kevin had more than 25 years of experience providing advice and counseling regarding the laws, regulations, policy and politics pertaining to export control, sanctions, national security reviews of foreign direct investments and other international trade issues. Previously, he served as the Assistant Secretary of Commerce for Export Administration from 2010 to 2017 with the Bureau of Industry and Security where he developed and implemented policies pertaining to export administration issues. Kevin, thank you so much for returning to testify again today.

Next, we have Giovanna Cinelli, Fellow at National Security Institute at George Mason University Antonin Scalia Law School. Throughout a career spanning over 30 years, she has represented and counseled defense, aerospace, financial, private equity, software services and high technology companies on a broad range of issues affecting national security including export investigations, due diligence, sanctions and sanction-related policies, Post-Transaction Cross-Border Compliance Committee on Foreign Investment in the United States reviews, government contracts, export policy and licensing. Ms. Cinelli has also served as a Naval Reserve Intelligence officer, so thank you for coming today.

Finally, we will hear from David Hanke, also a Fellow at National Security Institute at George Mason University Antonin Scalia Law School. While working on Capitol Hill, he was the primary staff architect of the Foreign Investment Risk Review Modernization Act and the chief strategist behind its 2018 enactment. Beyond the Committee on Foreign Investment in the United States, he also advises companies on U.S. government policy regarding supply chain and strategic technology issues such as 5G telecommunications infrastructure and domestic semiconductor manufacturing. And he helps clients interface effectively with federal agencies and Congress. Thank you for coming today, Mr. Hanke.

Kevin, we are going to begin with you. We advise all the panelists to try to keep their remarks to seven minutes so we have ample time for a question and answer and appreciate your coming before the Commission today.

OPENING STATEMENT OF KEVIN WOLF, PARTNER, AKIN GUMP

MR. WOLF: Great. Happy to be here. I'll skip the three-hour version. The -- I have one -- and a three-day version, as you may have known.

Anyway, so thank you for asking me to testify today. I'm here on my own behalf. I'm not speaking on behalf of others. The views are my own.

And the main point is that, never before -- and I've been doing this 30 years -- have export controls been as complex and serious as they are now. And it's primarily the result of Chinese technology acquisition and use efforts that are contrary to our interests.

Also, the rapid pace in evolution of commercial technologies outstripping bespoke military technologies and complex supply chains make it even more difficult.

I can also say that the multilateral export control regime process which is critical to U.S. objectives, as discussed during the previous past session, was not designed to, and does not now, address unique national security issues created by China -- Chinese technology acquisition efforts that are not related to traditional Weapons of Mass Destruction, military space items or the parts, components, technology or software that are necessary for their development or production.

And so, sort of to make my main point differently is that there's an active public discussion about what the role and purpose of export controls are. And outside of the traditional WMD nonproliferation objectives.

All sorts of ideas are being discussed but -- such as dealing with strategic or breakout competitions, supply chain security, military civil fusion policies involving widely available commercial technologies, intellectual property theft, technology leadership issues, efforts to promote democracy over authoritarianism and the misuse of commercial technologies in the commission of human rights abuses. But these are all, obviously, critical U.S. policy objectives, but the regimes define and bound the contractual control systems of our allies.

And you heard in the previous session a really good discussion about the, you know, the drawbacks of unilateralism. Nevertheless, because of the serious issues that Chinese technology efforts -- acquisition efforts create, there's a tension for U.S. policy makers between wanting to move quickly and to impose unilateral controls that are initially effective but eventually, in most cases, but not all cases, counterproductive.

And then the multilateral process, the traditional process, which is eventually effective because more countries are imposing the same controls but are either very hard or time-draining to get there.

Or if the national security objective to be addressed is outside the scope of the traditional regime mandate, then the laws of our allies simply do not allow for their countries to impose similar controls.

The U.S., as a result of ECRA, that's been referred to, has extraordinary discretion -- in fact, a Congressional mandate for unilateral controls or end use controls or end user controls in certain circumstances.

But that authority doesn't exist among our allies. So since this is a -- I have a much longer written document I would refer you to, but I have basically five primary recommendations for you all.

And the first recommendation is somebody needs to come up with a definition of what national security means outside the context of the traditional, nonproliferation objectives of export controls.

There are lots of ideas that are being tossed about. Everybody goes straight to control this or control that, but nobody is defining what the objectives of the new control is.

And I go back to, with my experience in the government when I was given an instruction, for national security reasons, to fundamentally reform the export control system.

Secretary of Defense Gates gave a speech very early in the administration that laid out, very explicitly, what national security meant with respect to defense trade with our close NATO allies.

And so, for seven years, our instruction was to implement, through rule changes, that very clear mission at the beginning. And in order to know what to do, to address those seven topics that are outside the traditional nonproliferation objectives, somebody -- and I would hope and expect this could be a bipartisan objective that the administration should lead, should define what that term means in this context.

And in fact, ECRA was set up to precisely give the administration the discretion and the requirement to do so outside of the traditional regime approach. And then once that is done -- once there's somebody who can articulate in an actionable way a definition of what national security means outside the traditional nonproliferation objectives, then you work with the allies and you convince them that they're -- with that evidence, with that advocacy, with this new definition, with an appeal to common interests and other incentives that there needs to be a fundamental rethinking of what the purpose and use of export controls is to deal with the China issues.

And ECRA creates the standards and the authority for that. So there isn't new law that's needed to accomplish that. It's all set up already for the administration to accomplish.

But you don't have to wait until convincing the allies to change their rules to give themselves as much regulatory flexibility for list space and user and end use controls. A great deal can be done in the short term of coordinating with the allies on licensing policies and enforcement information on already controlled items. And I suspect that's already happening now, and it's not a new issue but it's something where there could be a lot of progress in the short term.

The third primary recommendation I have is with respect to the emerging foundational technology process. Frankly, it needs massive more resources to do it. There are lots of experts in the government at electronic warfare and other proliferation objectives, but there simply aren't the people in the government who know this area well enough to be able to understand the questions to be able to identify the choke-points, I think.

A lot of really terrific experts, but remember, the U.S. Export Control System and the allied export control system was not built to achieve and to address the issues that are being discussed today.

And ECRA basically started that process, which was terrific bipartisan legislation.

The last two points, because I know I'm running short, is I have a longer speech about the need for using export controls to address human rights objectives.

That's something that was always a little bit part of the system, but I believe now, with change of use of commercial technologies, it should be a much more aggressive effort.

Now that's something for which you should proceed unilaterally given the moral imperative of the objective. But remember to do so carefully given that you're going to be

dealing with widely available technologies, and the controls would need to be focused on -- in uses, not just particular items.

And then my final point in my last ten seconds is don't forget about the rest of the planet. There's a whole other planet -- I mean, there's a whole other planet.

I mean, there's a whole system dealing with proliferation-related items and the regular work of BIS. And that can get lost in the bright lights of trying to deal with all these China topics. And I'm not saying take the focus off of China, but please don't forget the rest of the planet. Please don't forget the rest of BIS's mission.

Please try to get to and support BIS and the agencies to get to a system where they can process regulations and licenses and decisions quickly, within the time period set out. Yeah, so I'll stop there and thanks for inviting me. And I look forward to our discussion later.

PREPARED STATEMENT OF KEVIN WOLF, PARTNER, AKIN GUMP

Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "U.S.-China Relations in 2021: Emerging Risks"
Panel III: "Assessing Export Controls and Foreign Investment Review"

The Honorable Kevin J. Wolf
Former Assistant Secretary of Commerce for Export Administration (2010-2017)
Partner, Akin Gump Strauss Hauer & Feld LLP

September 8, 2021

Vice-Chairman Cleveland, Commissioner Glas, and other members of the Commission, thank you for the opportunity to appear before you again. Although I am now a partner in the international trade group of a law firm, the views I express today are my own. I am not advocating for or against any changes to legislation, regulations, or policies on behalf of another.

Rather, given my background and desire to help the Commission's efforts, I am testifying about, and provide recommendations regarding, (i) the strengths and weaknesses of U.S. unilateral controls and the role of multilateral controls; (ii) the challenges of identifying emerging and foundational technologies warranting export controls; and (iii) what needs to be done to address China-specific threats to U.S. national security and foreign policy interests that can be accomplished through export controls. I am also willing to answer any questions about export controls during the hearing or in written responses later for the benefit of the Commission.

As a compliance attorney, Special Compliance Officer, and an Assistant Secretary responsible for administering and updating export control policies, regulations, and licensing systems, I have been working in the area for nearly 30 years. This means that I started my career about when the current export control system essentially began and have seen first-hand the evolution of the current technologies, threats, arguments, concerns, unintended consequences, and issues on a near-daily basis. From the government and industry sides of the issue, I have probably heard every argument and response to an export control topic. Although I am not a China- or any other specific-country policy expert, I am an expert in explaining, administering, developing, and implementing the rules governing the export, reexport, and transfer of commodities, software, technologies, and services in order to achieve national security and foreign policy objectives without unintended or counterproductive consequences. As these career comments suggest, I am also a true believer that export controls are a vital tool in advancing our national security and foreign policy objectives. Thus, I am grateful that you are holding this hearing and considering the issues so seriously.

In light of this background, I can say with confidence that never before have the issues involving the role of export controls been as complex and serious as they have been in recent years—mostly as a result of changes in the commercial technology acquisition and use policies in China. The rapid increase in the speed of commercial technology evolution, which far outpaces the development of traditional defense-focused

technologies, and ever-expanding global development and production supply chains make the issues even more difficult to handle.

I can also say with equal confidence that the multilateral export control system—which is critical to the success of U.S. objectives—was not designed to, and does not now, address Chinese government policies pertaining to commercial technologies that do not have a direct link to weapons of mass destruction (WMD), conventional weapons and other military items, space- and launch-related items, or the dual-use commodities, software, and technologies necessary for their development, production, or use. With respect to such items, the U.S. and its allies already have robust controls and well-tested regular processes for updating the lists of such items. The global pandemic has limited such efforts in the last 18 months and, as with all systems, there are ways to make it work better. There is nonetheless a system with standards that has generally worked well for 30 years or so. Moreover, the U.S. has had for decades complete embargoes on exports to China of all commodities, software, and technologies bespoke for military-, launch-, or space-related applications, regardless of significance. Thus, my comments today are about all other items that are not within these existing controls.

To make my main point differently and in terms of the current public discussion in the United States about how export controls could be used in new ways to address China-specific policy issues, the multilateral export control regimes—and thus the domestic export control laws of our allies—do not have, with rare exceptions, the mandate or legal authority to address:

i. strategic or great-power competition issues;

ii. supply chain security;

iii. military-civil fusion policies involving widely available commercial technologies;

iv. intellectual property theft;

v. technology leadership objectives;

vi. efforts to promote democracy over authoritarianism; or

vii. the misuse of commercial technologies to commit human rights abuses.

These are all, of course, critical issues warranting U.S. policy responses. With rare and modest exceptions, however, only the United States has broad legal authority to use export controls to accomplish more than traditional non-proliferation objectives. This authority comes from the Export Control Reform Act of 2018 (ECRA), which was a perfect example of bipartisan efforts to develop good law to address contemporary issues.

There is therefore a tension for U.S. policymakers between the desire to use export controls to respond quickly to Chinese state policies contrary to our interests and the reality that, with rare exceptions, history has shown that unilateral (U.S.-only) controls are usually *eventually* counterproductive. (There are exceptions that I will mention later.) This is the case because when allied countries do not have the same controls, income and investment flow to the companies in those countries that develop and produce the technologies at issue, which then supports their R&D efforts to out-innovate competitors in the United States that cannot get that income—and the country of concern is not deprived of the items of concern. (Most of the technologies of concern evolve quickly, which means that massive amounts of R&D are needed to develop the next versions to stay competitive.) Thus, the U.S. industrial base is harmed, foreign competition benefits, and the countries of concern are not hurt.

To put it more simply, unilateral controls are quick and responsive, but are usually *eventually* counterproductive and ineffective. Multilateral controls under the current system are *eventually* effective, but are either slow in creation given the need for regime member consensus or impossible, if not based on traditional, destination-agnostic non-proliferation objectives. Congress was well aware of this fact when it wrote in ECRA's primary policy statement (in sections 4811(5) and (6)) that:

> Export controls should be coordinated with the multilateral export control regimes. Export controls that are multilateral are most effective, and should be tailored to focus on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States and its allies.
>
> Export controls applied unilaterally to items widely available from foreign sources generally are less effective in preventing end-users from acquiring those items. Application of unilateral export controls should be limited for purposes of protecting specific United States national security and foreign policy interests.

Because unilateral approaches are eventually counterproductive and the traditional multilateral regime approach is neither quick nor responsive, the medium- and long-term solution to addressing the issues of this hearing must be aggressive, well-supported efforts to work with smaller groups of close allies in the producer nations of the technologies of concern to convince them to (i) expand the scope of their domestic export control laws and (ii) align their licensing and enforcement policies based on new, common understandings of the purpose of export controls. I suspect some form of these efforts is already underway, but I do not know the details. In any event, in my view, the highest export control policy priority of the Administration (and Congress in an oversight role) should be in the pursuit of this effort—i.e., doing the work necessary to convince the allies in producer nations to agree to a new paradigm and role for export controls to address, to the extent possible, the threats of common concern I listed earlier, as well as traditional proliferation-related threats.

The short- and medium-term solution with respect to regulatory changes is to provide financial and other support to the Administration's emerging and foundational technology identification and control process *consistent with the standards set out in ECRA*. Congress should be vigilant in its oversight and funding of such efforts, but patient in expecting immediate results from a new Administration because both will require months of daily effort by many people to succeed. I have read the USCC paper and other letters asking for quicker action. Clearly, Congress inserted the section into ECRA so that the Trump and future administrations would identify and control emerging and foundational technologies essential to national security that were not controlled by the traditional regime process. As to what was or was not done to satisfy this obligation in an August 2018 statute, I will have to defer to government officials to explain.

Since the purpose of this hearing is to consider recommendations, I have the following suggestions for how to do this.

1. **The Administration should develop (with bipartisan input from Congress), and a senior Administration official should announce, an actionable definition what "national security" means in the context of using export controls to address China-specific policies that are outside the scope of traditional non-proliferation objectives.**

2. **The Administration should advocate and support with evidence and appeals to common interests the adoption of that definition by a smaller group of close allies in countries that produce the core technologies of concern to convince them to (a) expand their legal authorities to impose controls for reasons not related to traditional non-proliferation objectives and (b) align their China- and other country-specific licensing policies and enforcement priorities for already-controlled items.**

3. **At the same time and with the same degree of intensity, Congress and the Administration must provide clear direction, robust funding, and political support to the export control agencies to implement the objectives of ECRA's emerging and foundational technologies provision based on the (a) the standards and process set out in ECRA and (b) agreed-upon definition of "national security" to address threats outside the context of traditional non-proliferation-related concerns.**

4. **Export controls should absolutely be used more to address human rights issues in China and elsewhere, but the Administration will need to include carefully crafted end use controls because the technologies at issue will generally be widely available commercial items that are not subject to any multilateral controls.**

5. **Without taking away from the seriousness of the China-specific issues, Congress and the Administration should remember to give adequate attention and resources to all other export control issues, such as (a) running an efficient licensing system, (b) controlling and enforcing the export of dual-use items that have proliferation-related uses elsewhere in the world, and (c) reducing unnecessary barriers on controlled trade with close allies.**

The following provides more detail and support for each recommendation.

1. **The Administration should develop (with bipartisan input from Congress), and a senior Administration official should announce, an actionable definition what "national security" means in the context of using export controls to address China-specific policies that are outside the scope of traditional non-proliferation objectives.**

This is a corollary to the first rule of regulatory and legislative drafting, which is to clearly define the problem to be solved in order to know what the regulation or legislation prohibits or requires. There are many threads of good ideas floating around within the Administration and on the Hill. The Administration, however, needs to take the lead at articulating and getting general bipartisan acceptance of a clear, common vision as to the purpose and scope of China-specific export controls and export control policies to address issues outside the traditional non-proliferation-related concerns.

No new legislation or Executive Orders are needed to accomplish this recommendation. The legal authority for the effort already exists in ECRA. A senior Administration official from, for example, the National Security Council or the Cabinet, should articulate the consensus Administration position on what "national security" means with respect to the need to control China items that do not have traditional proliferation-related applications. (The text could be, for example, a detailed Statement of Conclusions agreed to at a Principals Committee meeting or included in an interagency-cleared speech to a major organization.) The example I have in mind as an analogy to this suggestion is the speech Secretary of Defense Gates gave early in the Obama Administration that set out the vision for and the national security objectives of the Export Control Reform effort. It guided our efforts and mission for the next seven years. When in doubt as to whether the effort was on the right track or what "national security" meant in the context of Export Control Reform (which is very different than the current issue), we referred back to the principles in the speech and the follow-on instructions.

In other words, someone in the Administration needs to decide and then announce in a way that will guide for years the actions of the export control agencies whether and to what extent unilateral, plurilateral, or multilateral controls on the export, reexport, and transfer of *specific* commodities, software, technology, and services could—or could not—be *effective* in addressing (i) strategic or great-power competition issues, (ii) supply chain security, (iii) military-civil fusion policies involving items not directly related to proliferation-related items, (iv) intellectual property theft, (v) technology leadership

objectives, (vi) efforts to promote democracy over authoritarianism, and/or (vii) the misuse of commercial technologies to commit human rights abuses. If export controls could not be effective at addressing such issues, then they should decide and announce that they will be addressed through other regulatory or legislative vehicles.

Export controls do not exist for their own sake. They are a means to an end. Each of these seven topics could and should be the subject of its own hearing and position papers to analyze how or whether new export controls could be effective—i.e., to have the desired result for the issue without *unintended* adverse collateral consequences. I highlight here "unintended" because all export controls have economic consequences. That is their point—to block or regulate the flow and sale of items to achieve other objectives. To know whether such consequences are *intended*, however, one must first have a clear definition of the end to be achieved.

Without a clear, detailed vision, there cannot be clear, effective identification and implementation of new controls (or licensing policies for already-controlled items)—only the creation of uncertainty, which history has shown is harmful to beneficial trade and investment. Without such a definition, there also cannot be a clear or persuasive policy basis to use to convince the allies in producer nations of key technologies to think differently about their export control policies, laws, regulations, and enforcement priorities.

For example, when the goal is controlling that which is necessary to make a missile, experts research which bespoke and dual-use components, software, and technologies are necessary to develop, produce, and use missiles. That list of items then becomes what the allies agree to control for missile technology reasons. When the China-specific concern is an issue that is not a missile or another obvious proliferation-related end item, there must first be an equally clear definition of the goal in order to know the cut lines for specific technologies to control. With every technology area, there are thousands of variations and generally complicated international component supply chains. This means that the definition of the problem to be solved must be clear enough to allow for the detailed identification of items that are specific to that problem given the reality of modern, global production of most commercial items.

Although some will see this recommendation as simple (or even obvious), I nonetheless make it here because it (i) is critical to the success of all other efforts; (ii) was not done by Congress or the Trump Administration; (iii) has probably not yet been done by the Biden Administration; (iv) **is usually forgotten in public discussions about imposing new export controls**; and (v) will be massively hard to accomplish for any administration. Getting to an answer must be process- and fact-driven because no one person or agency has all the answers. For example, if a particular national security objective is to address an economic issue, such as a strategic competition issue, then unusually complex economic and global supply chain issues must be understood to know where the levers of controls are—and what the consequences would be of using controls to restrict trade in these items. Few in industry understand these levers and even fewer in the government do. This is why it will be critical for Administration officials

to work closely with academics, economists, trade and supply chain experts, and industry technology experts to gather information about, for example, what the "chokepoint technologies" are to achieve such objectives.

I recognize the dilemma in what I recommend. If the Administration is too explicit regarding what it plans to control over a long timeline, the industries affected will be inclined or instructed to leave the United States. They may also be inclined to invest in more development and production of such technologies outside the United States to not be caught behind the anticipated wall of expected new unilateral controls. This export control Heisenberg Effect is why I counsel congressional patience and understanding if Administration officials are sometimes publicly vague in their articulation of plans until they are completely ready to be announced.

I also recognize that developing this definition will be a far harder exercise than any traditional export control effort. The U.S.-China relationship is as complicated as it gets, and the technologies and supply chains at issue are even more complicated. Once an export control policy debate becomes unmoored from its traditional objectives regarding relatively identifiable WMD, military- and space-related applications, and the dual-use items necessary for their development, production, or use, then we are in uncharted waters. Notwithstanding the politics of the day and that this must be an Administration-led effort, I honestly believe that a bipartisan consensus on the definition is possible. The passage of ECRA and FIRRMA, and the likely passage of industrial policy legislation to address China-specific issues, are proof of this.

2. **The Administration should advocate, and support with evidence and appeals to common interests, the adoption of that definition by a smaller group of close allies in countries that produce the core technologies of concern to convince them to (a) expand their legal authorities to impose controls for reasons not related to traditional non-proliferation objectives and (b) align their China- and other country-specific licensing policies and enforcement priorities for already-controlled items.**

With rare, tailored exceptions that I will discuss later, for China-specific and other novel export controls not tied to traditional non-proliferation objectives to be effective, we need our allies to have the same controls. It is that simple and logical. When more countries control the movement of the same types of items for the same end uses and end users of concern, the controls are more effective. The export control systems of our allies, however, are essentially limited to regulating (i) weapons of mass destruction, (ii) conventional military items, and (iii) dual-use commodities, software, and technology that have some identifiable relationship to their development, production, or use. The lists of such items are determined by consensus in the four primary voluntary multilateral regimes, which are the Nuclear Suppliers Group (NSG), the Australia Group (AG) (for chemical and biological-related items), the Missile Technology Control Regime (MTCR), and the Wassenaar Arrangement (WA), which covers conventional arms and dual-use items to prevent "destablising accumulations" of such arms and their

acquisition by terrorists.

Moreover, the Wassenaar Arrangement has the following specific criteria for the types of dual-use items that should and should not be controlled:

> Dual-use goods and technologies to be controlled are those which are major or key elements for the indigenous development, production, use or enhancement of military capabilities. For selection purposes the dual-use items should also be evaluated against the following criteria:
>
> • Foreign availability outside Participating States.
> • The ability to control effectively the export of the goods.
> • The ability to make a clear and objective specification of the item.
> • Controlled by another regime.
>
> Those items from the Dual-use List which are key elements directly related to the indigenous development, production, use or enhancement of advanced conventional military capabilities whose proliferation would significantly undermine the objectives of the Wassenaar Arrangement.
>
> N.B. 1. General commercially applied materials or components should not be included.
>
> 2. As appropriate, the relevant threshold parameters should be developed on a case-by-case basis.
>
> Those items from the Sensitive List which are key elements essential for the indigenous development, production, use or enhancement of the most advanced conventional military capabilities whose proliferation would significantly undermine the objectives of the Wassenaar Arrangement.
>
> N.B. As appropriate, the relevant threshold parameters should be developed on a case-by-case basis.

The regime-listed items are destination-agnostic, meaning that they are created not with particular country issues in mind, but whether they have some inherent and identifiable relationship to a WMD or a conventional military item. Moreover, none of the regimes' mandates include the contemporary China-specific policy issues I mentioned earlier, where export controls are being considered as part of a solution.

The export control laws of our allies are largely based on and limited by the scope of the controls, and purposes for controls, in the multilateral export control regimes. This means that, after or while completing the definition of "national security" described in the previous recommendation, the United States needs to lead a robust and well-staffed diplomatic and technical effort to reach agreements among the export control communities and the relevant allied government authorities. We need to convince them

that the global, allied export control system is at an inflection point. We, the allies, need to collectively come to a new definition of common security interests and purposes for regulating the movement of commodities, software, technology, and services not directly connected to proliferation-related applications for specific destinations, end uses, and end users.[1]

I need to do more thinking and research before suggesting that the scope of the Wassenaar Arrangement could be expanded to deal with more than its traditional mandate. My sense is, however, that such efforts would fail given the need for consensus among the members—one of which is Russia—for change. I am also not suggesting the creation of a new multilateral regime to address the new export control issues being discussed. The groupings of the producer nations of each of the various technologies of concern require a complex Venn diagram to explain. The Bureau of Industry and Security (BIS) published in 2018 a list of emerging technology topics to be reviewed in response to the ECRA requirement to do so. It includes diverse areas such as biotechnology, artificial intelligence, advanced semiconductors, quantum computing, and additive manufacturing. There is no one international organization or group of countries with material development in all the technologies. Thus, the approach should be to work within existing international arrangements created for other reasons and to create *ad hoc* working groups of allied countries on a technology-by-technology basis, based on the priority of the issues and the technologies their companies produce. For example, one group of countries could be focused on semiconductor issues. Another group could focus on aerospace issues. A different circle of countries would focus on biotechnology issues. Such an approach is loosely referred to here as a "plurilateral" approach. (The exact method of doing this and which countries should be involved with which technologies will need to be subject of a separate paper.)

The United States led the efforts to move from the Cold War-era COCOM-based export control system to the multilateral regime-based system that we have now. It could lead a similarly large, transformational effort again. It will be hard, time-consuming, and require evidence, interagency cooperation, diplomacy, leadership, intelligence assessments, economic analyses, technical understanding of "chokepoint technologies," and thorough understandings of the allies' laws, policies, and politics. (As explained below, there are two different types of "chokepoint" technologies—those that are necessary to develop or produce proliferation-related items and those that are, or are necessary to develop or produce, the emerging and foundational technologies within the scope of ECRA section 1487.) Given our success in completing transformational efforts in the past, I believe that it is indeed possible—and, again, necessary—for new China-specific, plurilateral export control efforts to succeed. "Success" in this context means the existence in multiple countries of new controls to accomplish the agreed-upon national security goals described in the previous recommendation, once defined.

[1] The existing end use (e.g., the military end use rules) and end user (e.g., the Entity List) controls in U.S. law are complex. A full description of such controls, how they are different, and how effective they are will need to be addressed in a separate paper if requested.

In addition to focusing on the new standards for identifying and controlling additional types of commodities, software, and technologies, the allied government outreach should advocate their adoption of domestic "catch-all" laws enabling controls over exports of otherwise unlisted items to specific end uses and end users for reasons not tied to traditional WMD proliferation-related issues. For example, no other country has the authority the United States has to impose controls over the export of otherwise uncontrolled items if destined to a military end user in China, or for specific end users unrelated to WMD or terrorism (e.g., to many of those on the Entity List).

Convincing a small group of allies (and then later more) to agree to a paradigm shift in thinking about export controls to address China-specific issues will be particularly difficult because economic objectives have historically deliberately been excluded from multilateral export control policy discussions. Export controls were never originally intended to be used as a tool of trade protectionism or a tool to pick economic winners and losers. The focus of international export control policy discussions over the decades has been about whether a particular commodity, software, or technology had inherent proliferation-related applications agnostic of the economic or other policies of any particular country. Controls were not imposed because they would economically benefit or harm particular companies or sectors. Licensing decisions were not based on whether there would be a loss of profit for a sale that would have proliferation-related implications. Such views remain solid in the minds of export control policy officials in allied countries. As well described in the justifications for the industrial policy bills being considered in Congress, Chinese government policies to artificially subsidize key technology sectors in order to achieve strategic dominance over U.S. and allied competitors are forcing new thinking in the United States on such issues. Just as the United States once eschewed industrial policy, it needs to begin to factor in—and convince the allies to factor in—economic considerations of common interest when deciding what should be controlled and how.

Immediate Benefits from the Effort

What I am advocating will take years of diplomacy and advocacy to accomplish, even with sufficient resources devoted to the effort. Legislation and long-held policy views on complex issues in all countries change slowly. This does not mean that there cannot be immediate benefits from such outreach efforts. Under the existing multilateral export control process, each member country has significant (although not complete) national discretion to make its own licensing policies and set its enforcement priorities. Thus, there is a lot of room for the United States and relevant allies to work together to share information about particular exports of already-controlled items, end users, and end uses as part of efforts to align, formally or informally, licensing policies. This has always been part of BIS's mandate, so this is not a new suggestion. However, I am advocating increased Administration attention to, and congressional support for, such efforts. They will not only make controls pertaining to China and other countries more effective, they will also level the playing field for U.S. industry relative to their foreign competitors.

Another benefit of such informal and plurilateral efforts is that core Wassenaar member

countries can work together to get alignment on new types of items that should be multilaterally controlled. I realize that the Wassenaar Arrangement has significant formal limitations on what is within the scope of its mandate, but the definition of the key terms of this mandate is up to the members' discretion. If enough core members come together and work out in advance proposed new controls on particular technologies, it is possible that non-producer member countries will not be concerned with, oppose, or notice proposed new controls that push traditional Wassenaar control boundaries. This is, however, hard to predict in advance given the dynamics of an organization that has 43 diverse members, including Russia, where consensus is required to change the lists of controlled items. (This is both the virtue and vice of large multilateral organizations.)

Congress can help with such efforts by supporting or requiring, in the appropriate legislative vehicles, the Executive Branch to reach out to the key allies to do the work necessary to convince them to expand the scope of their export control laws and to work together with respect to existing controls. Such efforts would be consistent with congressional calls during the creation of FIRRMA for the administration to reach out to the allies to convince them to adopt their own or expanded foreign direct investment rules. Specifically, it was the sense of Congress (in section 1702(b)(2)) that the "President should conduct a more robust international outreach effort to urge and help allies and partners of the United States to establish processes that are similar to the Committee on Foreign Investment in the United States to screen foreign investments for national security risks and to facilitate coordination." By most accounts, such efforts were and continue to be quite successful. In addition, Congress could fund an ongoing study to be conducted and regularly updated that describes, compares, and contrasts the details of the export control and foreign direct investment rules of our allies. Such information would be extremely helpful to the success of the effort because policymakers will know what already exists and what would need to be changed.

Finally, the Administration will need to be careful to speak with one voice when conducting such outreach with the allies. It is easy and natural, in any administration, for different agencies to vary in how they characterize a complex objective. This is why a clear articulation of the definition of "national security" in this context, as described above, is a prerequisite. By way of analogy, all allied outreach efforts to describe the Export Control Reform effort were, for the first several years, always conducted jointly by representatives from Defense, State, and Commerce. In this way, there was no risk that one agency was going in a different direction, which would harm the effort. Eventually, after hearing each other's presentations so many times, we got comfortable enough that all agencies were on the same page, had the same message, and were even telling the same jokes that we did not need to do joint presentations in the latter years of the effort. Such a China-focused outreach will, however, be more sensitive for some allies that may not want it immediately known that they are working with the United States on such efforts. So, I counsel patience with respect to requests for some allies to publicly commit to supporting the effort before it is completed.

3. At the same time and with the same degree of intensity, Congress and the Administration must provide clear direction, robust funding, and political support to the export control agencies to implement the objectives of ECRA's emerging and foundational technologies provision based on the (a) the standards and process set out in ECRA and (b) agreed-upon definition of "national security" to address threats outside the context of traditional non-proliferation-related concerns.

ECRA's Traditional Export Control Policy Provisions—Section 4811

ECRA Section 4811 sets out the traditional, and still critical, purposes of U.S. export controls. It is basically a codification of the export control policies of previous administrations and Congresses. Please take a moment to read it. It is what a bipartisan Congress and the Trump Administration agreed to as the purpose of U.S. export controls[2] just three years ago (to replace a 1979 statute that had lapsed for decades because of an inability of Congress and the Administrations to reach a consensus statement of U.S. export control policy in law). I and many others—Democrats, Republicans, hawks, doves, and owls—supported it. The core policy provisions are the following:

The following is the policy of the United States:

(1) To use export controls only after full consideration of the impact on the economy of the United States and only to the extent necessary—

(A) to restrict the export of items which would make a significant contribution to the military potential of any other country or combination of countries which would prove detrimental to the national security of the United States; and

(B) to restrict the export of items if necessary to further significantly the foreign policy of the United States or to fulfill its declared international obligations.

(2) The national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specific activities of United States persons, wherever located, be controlled for the following purposes:

(A) To control the release of items for use in—

[2] Given that there are comprehensive arms embargoes on China, I am not referring to or discussing here the Arms Export Control Act or the export control regulations administered by the State Department or other departments.

(i) the proliferation of weapons of mass destruction or of conventional weapons;
(ii) the acquisition of destabilizing numbers or types of conventional weapons;
(iii) acts of terrorism;
(iv) military programs that could pose a threat to the security of the United States or its allies; or
(v) activities undertaken specifically to cause significant interference with or disruption of critical infrastructure.

(B) To preserve the qualitative military superiority of the United States.

(C) To strengthen the United States defense industrial base.

(D) To carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy.

(E) To carry out obligations and commitments under international agreements and arrangements, including multilateral export control regimes.

(F) To facilitate military interoperability between the United States and its North Atlantic Treaty Organization (NATO) and other close allies.

(G) To ensure national security controls are tailored to focus on those core technologies and other items that are capable of being used to pose a serious national security threat to the United States.

(3) The national security of the United States requires that the United States maintain its leadership in the science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation. Such leadership requires that United States persons are competitive in global markets. The impact of the implementation of this subchapter on such leadership and competitiveness must be evaluated on an ongoing basis and applied in imposing controls under sections 4812 and 4813 of this title to avoid negatively affecting such leadership.

(4) The national security and foreign policy of the United States require that the United States participate in multilateral organizations and agreements regarding export controls on items that are consistent with the policy of the United States, and take all the necessary steps to secure the adoption and consistent enforcement, by the governments of such countries, of export controls on items that are consistent with such policy.

As described in paragraph 10 of ECRA section 4811, “export controls complement and

are a critical element of the national security policies underlying the laws and regulations governing foreign direct investment in the United States, including controlling the transfer of critical technologies to certain foreign persons." Based on the congressional testimony and statements that were part of the effort to create and pass ECRA and the Foreign Investment Risk Review & Modernization Act (FIRRMA), this, of course, was largely referring to Chinese state policies of concern and not limited to traditional non-proliferation-related objectives.

The last sentence of paragraph 10 is thus key to this hearing. It states that **"[t]hese efforts should be in addition to traditional efforts to modernize and update the lists of controlled items under the multilateral export control regimes."** Congress required that such technologies be identified not only for the sake of knowing what additional export controls should exist but also to create more mandatory filings with CFIUS for non-controlling investments where such technologies could be disclosed to foreign persons as a result. Thus, export controls and U.S. foreign direct investment controls are aligned in this regard.

ECRA's Emerging and Foundational Technologies Provisions—Section 4817

To implement and bound such efforts "in additional to traditional" regime efforts, Congress created section 4817—the emerging and foundational technologies section. It requires the Administration to conduct a "regular, ongoing interagency process to identify emerging and foundational technologies that . . . **are essential to the national security of the United States" and not described in any of the existing export control regimes.** That's the entire standard. It is much shorter than section 4811, but potentially much broader in scope. Congress deliberately did not define what "national security" means in this context—i.e., to address China-specific issues outside the scope of the traditional regime controls. It left that up to the successive administrations to do, presumably because the concerns would shift over time. Also, defining national security in specific situations is a normal function of the Executive Branch. **Defining "national security" in this context outside traditional proliferation-related objectives is thus a key export control mission of the Biden Administration and future administrations—and the central regulatory issue with respect to the purpose of your hearing today.**

To identify such technologies, Congress required the administration to draw upon all available resources for such information, including the intelligence community, industry advisory committees, and information CFIUS received or developed as part of its review of cases. Congress made this point recognizing that the economic and technical issues associated with such technologies are unusually difficult to understand and that they evolve quickly. As good as government staff in the agencies are, they will not always have such information, particularly if it relates to novel technologies unrelated to those of proliferation concern. Thus, if BIS or any other export control agency does not have the staff or expertise to analyze or identify a particular technology, Congress has required the agency to reach out to others for help.

To use my missile control analogy, it is relatively easy to take apart a missile and determine which parts, components, technologies, and software are directly related to its development, production, and use. The need to control missiles is also obvious, regardless of foreign availability and the economic implications of denying exports. It is massively harder to "take apart" the emerging technology topics of the day, such as "artificial intelligence" and "quantum computing." They are not always just things. They are in large part global collections of know-how using widely available items being created and moved across boundaries on a daily basis.

Thus, identifying precisely those core chokepoint components, software, and technologies that meet the ECRA standards for such items is massively harder and requires more resources and creativity than anything that has ever been done in the export control system. **To repeat, until there is a clear, common, and understood definition of "national security" in this context, one cannot know what to look for to identify and control "emerging" and "foundational" technologies.** Just because a technology is emerging does not necessarily mean it warrants control. Just because a technology is basic does not necessarily mean that it does not warrant control. One must know the goal of the control first. And until one knows the definition of "national security" in this context, one cannot know if BIS is moving too slow, too fast, or just right with respect to the identification of "emerging" and "foundational" technologies.

In order to enable the Administration to move quicker than the multilateral system permits, but without creating counterproductive consequences, ECRA Section 4817 then requires the Administration to identify and impose unilateral controls over whatever the Administration defines as "emerging" or "foundational" technologies *so long as such efforts t*ake into account:

> (i) the development of emerging and foundational technologies in foreign countries;
>
> (ii) the effect export controls imposed pursuant to this section may have on the development of such technologies in the United States; and
>
> (iii) the effectiveness of export controls imposed pursuant to this section on limiting the proliferation of emerging and foundational technologies to foreign countries.

Thus, if a particular technology of concern is widely available outside the United States, then it is not a good candidate for unilateral controls under this section. This is logical because if a particular technology that does not have a clear proliferation-related use is widely available outside the United States, then imposing a control over it would not be effective. This conclusion is reflected in the second two elements of this limitation in section 4817(a)(2)(B), i.e., that if a unilateral control would harm domestic research in the technology or would not be effective, then it is also not a good candidate for a unilateral control. If the technology nonetheless warrants control based on the standards for control in ECRA, then the plurilateral or traditional multilateral approach

should be used.

As a double check on the process to ensure that there are not mistakes or unintended consequences, section 4817(a)(2)(C) requires any such unilateral controls to be published as proposed rules and subject to public notice and comment. The primary benefit of such efforts will be to gather information about whether there is material foreign availability for the technologies proposed for control. The government generally does not have a fraction of such information that is available to industry. Although industry is often limited in what it knows given that much of the information is proprietary to their competitors, it will generally still have more such information than the government. Thus, the need to collect, present, and understand foreign availability information in order to comply with this part of ECRA is particularly challenging and time consuming, but critical to the success of the effort.

Also, as someone who has written, cleared, negotiated, implemented, and interpreted hundreds of regulations, I speak with authority when I say that one must be humble when drafting and publishing export control regulations. Given their complexity, it is easy to make mistakes and create unintended consequences. Getting it right takes time. One must also have trust in the interagency and public notice and comment process, and the opportunity for others to double check your homework. Finally, tracking a process that I created in 2012 in the EAR to quickly and unilaterally control emerging and other technologies of concern, Congress gave the Administration (in section 4817(c)) three years to work with the regimes to get acceptance of the control by a multilateral regime or decide if a permanent unilateral control was consistent with national security interests.

For such new controls to have a possibility of becoming multilateral (and thus most effective), they will need to be written and presented in the specific types of control text of the relevant regime control lists. The Commerce Control List (CCL) of the Export Administration Regulations (EAR) is where in U.S. law the lists of agreed-upon multilateral regime lists are published. The CCL also identifies the commodities, software, and technologies that only the United States controls. Section 4817(c)(2) does not require the creation of a separate list of "emerging" and "foundational" technologies. Rather, it requires an "ongoing" process to add such items to the CCL (or U.S. Munitions List, if uniquely military). Indeed, to its credit, the Trump Administration implemented in the CCL more than 35 new controls on emerging technologies through the multilateral process, which are described in an October 2020 press release issued by Secretary Ross.

Although ECRA does not require separate lists of emerging and foundational technologies, clearly that is the expectation of many who follow this issue and ask about it on a regular basis. A way to address such reasonable expectations to know what has been identified under the authority of section 4817, while staying consistent with the organizational structure of the CCL, would be for BIS to identify which items on the CCL were added under the authority of the emerging and foundational technology provision of ECRA. For example, BIS could add an "EFT" or a "50 USC 4817" code note in the

Export Control Classification Numbers (ECCNs) on the CCL for such items. It could also create a separate web page on www.bis.doc.gov describing in one place the items that have been controlled under the section 4817 standards and process.

As to the "foundational" technology identification effort, BIS wrote the following when it published a request for public comments on the issue on August 27, 2020, which was more than two years after the passage of ECRA:

> There may be additional items, classified on the CCL at the AT level or as EAR99 for which an export license is not required for countries subject to a U.S. arms embargo that also warrant review to determine if they are foundational technologies essential to the national security. For example, such controls may be reviewed if the items are being utilized or required for innovation in developing conventional weapons, enabling foreign intelligence collection activities, or weapons of mass destruction applications. BIS, through an interagency process, seeks to determine whether there are specific foundational technologies that warrant more restrictive controls, including technologies that have been the subject of illicit procurement attempts which may demonstrate some level of dependency on U.S. technologies to further foreign military or intelligence capabilities in countries of concern or development of weapons of mass destruction.

I will leave it to BIS to comment on the status of such efforts and why it took more than two years to even ask for public comment on the statutory requirement. I do not know the answer. I do, however, know that if an administration needs more resources to satisfy such statutory requirements, then it needs to ask Congress for them. Because the China-specific issues being discussed today are a strategic priority for Congress, then it should grant such requests. Little more than regular cost-of-living budget adjustments for BIS, and the other export control agencies are insufficient. Setting aside for the moment the congressional mandate to conduct this effort and the budget issues, I nonetheless counsel patience and vigilance because identifying the subset of such technologies, which are generally widely available, will be difficult given the standards in ECRA section 4817 to not impose unilateral controls on widely available technologies.

4. Export controls should absolutely be used more to address human rights issues in China and elsewhere, but the Administration will need to include carefully crafted end use controls because the technologies at issue will generally be widely available commercial items that are not subject to any multilateral controls.

ECRA section 4811(2)(D) states that one of the purposes for U.S. export controls is to "carry out the foreign policy of the United States, including the protection of human rights and the promotion of democracy." Unlike the national security topics described above, ECRA does not say much more on the issue, although the authority provided is

broad. Nonetheless, as you may know, there have been various bills introduced that would require BIS to consider creating new controls to address human rights issues, such as those related to censorship or social control, surveillance, interception, or restriction of communications, monitoring or restricting access to or use of the internet, identification of individuals through facial or voice recognition or biometric indicators, and DNA sequencing. I strongly support such objectives as important new additions to the role and use of export controls.

Some of the bills would slightly amend ECRA to provide clear authority for the imposition of end use controls when list-based or end user-based controls would not be effective. If these provisions become law, they will be important authorities for BIS because, with some exceptions to be listed out, the types of items commonly used to commit human rights abuses are widely available commercial items that will not usually be controllable as such. Controls on exports of unlisted items for specific *end uses* with such items that violate human rights will need to be a regularly used solution. Because end use controls are, however, inherently difficult for industry to understand and implement in compliance programs, the new controls will need to be carefully crafted with a significant amount of beta testing with compliance professionals and prosecutors to make sure they will be clear, effective, and enforceable.

There appears to be efforts within BIS to conduct such a review with or without new law. Moreover, BIS states on its webpage that it is "actively engaged in formulating, coordinating, and implementing various export controls to counter the use of items subject to the [EAR] that could enable human rights abuses or repression of democracy throughout the world. These controls are a mix of list-based, end-user, and end-use controls, as well as specific licensing policies that allow review of transactions for concerns about human rights abuses and repression of democracy." Also, to their credits, both the Trump and Biden administrations have used export control tools to address human rights issues. The primary tool has been to add to the Entity List those that have engaged, or believed to have engaged, in human rights abuses associated with the Chinese government's brutal repression of the Uyghurs and other ethnic minorities in the Xinjiang region. Also to the Trump Administration's credit, it amended the EAR so that human rights considerations are applied to the review of essentially all license applications, even when the items to be exported are not controlled for human rights-related (i.e., "Crime Control") reasons.

The issues and the export control levers to address human rights issues are somewhat different than the national security issues described above. For example, unilateral human rights controls are usually appropriate regardless of foreign availability given the moral imperatives involved and the need to signal U.S. resolve on the issues to the international community and allies. Also, unlike with respect to the non-proliferation-focused regimes, there are no multilateral organizations with authority to identify and list for common control among allies specific commodities, software, and technologies of concern for human rights reasons. That is, there is no Wassenaar-like arrangement to address human rights concerns, except for some issues pertaining to surveillance and cyber intrusion technologies. Thus, I would encourage Congress to require the

Executive Branch to lead an effort to get allied support for a new regime to control commodities, technologies, software, services, and end uses that warrant common control to achieve human rights objectives. Because such an effort will take several years and significant resources to complete, I would encourage Congress to provide the Executive Branch with the resources and mandate to do so soon.

5. **Without taking away from the seriousness of the China-specific issues, Congress and the Administration should remember to give adequate attention and resources to all other export control issues, such as (a) running an efficient licensing system, (b) controlling and enforcing the export of dual-use items that have proliferation-related uses elsewhere in the world, and (c) reducing unnecessary barriers on controlled trade with close allies.**

This part of the USCC hearing is about export controls and, naturally, China. Most of the think tank, public, political, and press commentary about export controls pertains to China as well. This is natural given the seriousness and difficulty of the issues. The focus is not wrong. Nonetheless, I want to use this platform to respectfully ask those who are thinking about export control policies to do what can be done to support BIS and the other agencies in just running a normal, transparent, and timely export control licensing system, regardless of the policies on any particular item or country. There is literally a whole planet full of other issues.

Without a regular, reliable, timely, and predictable licensing system, U.S. exporters cannot be reliable, timely, and predictable partners with respect to items that should be approved for export based on the applicable policies. Daily industry compliance issues also involve far more than just individual licensing decisions. (Applying for licenses to export controlled items to specific countries or proscribed persons is a core regulatory *compliance* effort.) There is a regular need for outreach, training, guidance, interpretations, classification determinations, responses to disclosures, and jurisdictional determinations. Indeed, being the interface between national security equities and industry is a core reason why BIS—the Bureau of Industry AND Security—exists.

BIS and the other export control agencies are full of excellent, dedicated, and smart career civil servants. The focus on the day-to-day running of the system can, however, easily get lost in the bright lights of discussions about what the China-specific policies should be. These are not just my views as a compliance attorney and a former assistant secretary in charge of export administration. The final three core policy objectives in ECRA section 4811 for U.S. export controls are the following:

> (7) The effective administration of export controls requires a clear understanding both inside and outside the United States Government of which items are controlled and an efficient process should be created to regularly update the controls, such as by adding or removing such items.
>
> (8) The export control system must ensure that it is transparent,

predictable, and timely, has the flexibility to be adapted to address new threats in the future, and allows seamless access to and sharing of export control information among all relevant United States national security and foreign policy agencies.

(9) Implementation and enforcement of United States export controls require robust capabilities in monitoring, intelligence, and investigation, appropriate penalties for violations, and the ability to swiftly interdict unapproved transfers.

Also, ECRA section 4816 requires BIS to provide exporters, particularly small- and medium-size enterprises, with assistance in complying with the regulations. ECRA section 4825(b)(2) states that the export control agencies "should regularly work to reduce complexity in the system, including complexity caused merely by the existence of structural, definitional, and other non-policy-based differences between and among different export control and sanctions systems." ECRA section 4814(c) states that the licensing process "should be consistent with the procedures relating to export license applications described in Executive Order 12981." This Executive Order requires, and is the legal authority (as amended) for, the interagency review and appeal process, and the timelines for such efforts, that are set out in the EAR. Merely setting *and achieving* a simple goal for BIS and its fellow export control agencies to have the resources and processes in place to meet the license review and other deadlines in the EAR would be an amazing and good government accomplishment. Getting to a predictable licensing schedule would also do wonders for our economic security objectives—regardless of any particular license policies (e.g., approval or denial) toward any country.

For these and other reasons, Congress and the Administration should also devote substantially more resources and personnel to the export control agencies, namely BIS, the Defense Technology Security Administration (DTSA), the Bureau of International Security and Nonproliferation (ISN), the Directorate of Defense Trade Controls (DDTC), and the National Nuclear Security Administration (NNSA). (Eventually, the export control agencies should be combined into a single licensing agency and the rules should be combined into a single set of export control regulations with one list of controlled items, but that is a subject for another day.)

Setting the China-specific issues aside for the moment, the issues and technologies are more complex than ever and the need for multilateral cooperation, which is time-intensive, continues to be extremely important to the controls' effectiveness. Remember that the EAR regulates thousands of dual-use commodities, software, and technologies that are necessary for the development, production, or use of missiles, chemical and biological weapons, nuclear items, and conventional weapons. The need to control such items aggressively and effectively is more important than ever. Similarly, the EAR, as a result of the Export Control Reform effort, is the vehicle for implementing many of the national security objectives of the Obama Administration—which the Trump Administration maintained—with respect to trade in less sensitive defense items and commercial space-related items with NATO and other close allies.

These controls need regular updating and care for them to continue to be effective.

My personal view, that I can describe in more detail separately, is that each agency is understaffed when compared to its mission. Among other things, this leads to increased burdens and delays for industry, reduced time available for internal training of the agencies' employees, and the inability to keep the regulations current. Failure to keep the regulations current to novel threats does not advance our national security interests and harms our economic security. A renewed attention to supporting these organizations should also include efforts to educate the next generation of export control professionals and to motivate them to join the federal government. Decades of wisdom and collective memory will walk out the door when current senior career staff retire or otherwise leave the government. As evidence of my commitment to the area, I have a standing offer to any college student, law student, veteran, or anyone else seeking a career change to discuss ideas for how to make international trade regulatory compliance a worthwhile career choice in industry or in government. The demand and need for dedicated, trained trade compliance professionals are only going to grow.

Similarly, I would encourage more resources be devoted to export control-focused enforcement, particularly by the subject matter experts and special agents at BIS's Office of Export Enforcement (OEE). This will not only advance the national security and foreign policy objectives of the controls, but also help keep the playing field level for those companies that do the hard work necessary to comply with the regulations. Part of this funding should also be focused on capacity building for the enforcement agencies of our allies and better coordination with countries that have diversion hubs. In addition, there should be more resources dedicated to enhanced DDTC/BIS compliance coordination. This would help with investigations involving items subject to both the International Traffic in Arms Regulations and the EAR.

Conclusion

Thank you again for asking me to testify today. I am happy to answer now or later any questions you have on export control issues. I am serious when I say that I have a 3-minute, 30-minute, 3-hour, and 3-day version of each such answer.

OPENING STATEMENT OF GIOVANNA M. CINELLI, FELLOW, NATIONAL SECURITY INSTITUTE AT GEORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL

COMMISSIONER GLAS: Thank you so much, Mr. Wolf. And now we'll recognize Ms. Cinelli.

MS. CINELLI: Thank you. It's a pleasure to be here. Vice Chairman Cleveland, Commissioner Glas, Chairman Bartholomew and distinguished commissioners, I appreciate the opportunity to speak to you today and share some perspectives as a practitioner and someone who has worked with organizations who have spent 30 or 40 years trying to comply with the regulatory regime.

No one says that laws and regulations have to be simple. And as an attorney, everyone knows ignorance is no excuse, but that doesn't mean it has to be constantly complicated and inconsistent.

And unfortunately, we are seeing in both the export control arena and the foreign direct investment arena a number of inconsistencies that, while well-intended because they're trying to meet a number of different objectives, are clashing in a way that is actually working to make them ineffective as opposed to effective.

Now in looking at it from the perspective of needing to, for example, advise an organization about whether to get an export license or whether to submit a filing to CFIUS, the one point I would like to mention here is that the only certainty is uncertainty.

There is literally an inadequate, and to Kevin's point, the definitional contours sometimes are inadequate.

But when you look at the reasons why we have export controls and foreign direct investment laws, it's because this changing geopolitical and geostrategic situation counsels for a degree of flexibility and resiliency in being able to address the issues as they arise.

But at the same time, this creates a conundrum for the regulations and the laws because this makes them constantly reactive. And from the perspective of being as effective as possible, looking at it from a business and legal construct, one of the most important things is to know what I have to comply with and the circumstances under which I have to comply with it. It does not mean that someone has to spoon feed me. It does not mean that everything has to be written out completely and clearly. But it does mean that I need to have sufficient information to adequately know what is required of me, under what circumstances and how.

Given where we are today, even with the advances and updates of ECRA and FIRRMA, I think there are some gaps that make some of these tools less effective and that perhaps Congress would want to consider as well as the Commission.

In the second attachment of my testimony, I include a list of questions. I apologize. I didn't have a chance to deal with some of them, but these are questions that come up. And I think a few of them would merit some additional review by the Commission and perhaps some hearings and actions by Congress because they do demonstrate how these are all interconnected. So having mentioned the reactivity, and just to give you a short summary on the export control side, export controls are not new. They go back to the founding of this country and the current regimes that we have in place, both for the Export Administration Regulations, pre-ECRA and the International Traffic and Regulations go back into the 70s and even earlier into the 50s for some of the Arms Export Control Act. So they have been public. They have been known. They

have been implemented and there have been slews of regulations. So the information has been out there.

But the laws that were written in the 50s, let's say, were done with a broad brush approach because not only of the nature of the balance of threats inequities that was facing the country at the time but also because at that point, there were different levels of technology and to a certain extent, the diffusion of technology and its perishability.

I had a client tell me one time that technology is a perishable asset. If you don't buy it today, it's worthless tomorrow. Perhaps a bit of hyperbole, but I think it does make the point clear that what we were looking at in the 50s, let's say, and how we define things may not apply as it does today.

That does not mean, however, that there should not be clear guidance and laws and regulations. It also does not mean that there should not be circumstances where we take a lead and actually control while we consider.

Again, in my Attachment 2, I reference the question of what happens in some of the nuclear world where, under the Atomic Energy Act, you can have technology that it born restricted. It's then considered and assessments are made on how and under what circumstances it continues to be controlled or it doesn't need to be controlled.

And I think that the same can apply both for the current export control system as well as for FIRRMA and the foreign direct investment. With this background, it leads me to highlighting three potential solutions. Let me start first with one that FIRRMA identified in a number of hearings. And that is how technology is shared. Most people are familiar with the fact that I'm a company. I want to transfer technology to someone. I need to get a license. I may have a patent, trade secret, some form of documentation that I can share. But technology is an asset. And in the bankruptcy process, those assets become available, put into a pool and they're examined sometimes in the same way as we examine equipment or contracts or receivables.

Now understanding that that's how the bankruptcy system was established, longstanding as well has a venerable history, the bankruptcy courts right now are not necessarily equipped to manage the national security reviews that are required for those types of situations.
So one of the suggestions is to consider updated the bankruptcy code to bring additional resources and engagement between the bankruptcy courts and the executive branch with those agencies that have stakes and equities in defining national security for purposes of an assessment of the assets that are being transferred as well as with the intelligence world that is going to be examining who the potential bidders are.

There are a number of different concerns. You can have bridge financing where anyone can come in and under those circumstances there's no clearance. But the courts are not well versed in how to manage that.

The second consideration is Senator Cotton, in his Beat China report, made a recommendation that the Department of Defense be a permanent deputy vice chair to the Committee on Foreign Investment in the U.S. And that would help balance some of the equities in that process.

It is never a bad idea to have additional support. Flat organizations which Treasury and CFIUS currently seems to be structured as -- flat organizations sometimes suffer from resource gaps and by adding a deputy vice chair and one with an equity in the national security world could be helpful.

And then the last point that I'd like to make is the disentangling of ECRA and FIRRMA. This is probably a bit of an inflammatory comment, so please forgive me in advance. But the comment is disentangling not decoupling. And I apologize, I'm over time. If -- I'll quickly finish the thought. Disentanglement does not mean that the Commerce Department would be removed from its obligations to identify emerging and foundational technologies as critical technologies.

But what it does mean is opening the aperture to all the other legislative authorities that already exist, such as in the NDAA, one of which I cited in my testimony 1049, but there are others -- 242, 243 -- which have given already, over the last several years, to the Department of Defense the remit to identify emerging technologies expressly linked to all the different multilateral missions that exist -- not just national security in the U.S. but power projection, like export licensing and foreign policy considerations.

It would be interesting and helpful if Congress would look at those authorities and consider how they best can be implemented and used by the interagency type processes, understanding that someone always has to make a decision.

You know, CFIUS has a chair; the interagency committees have chairs under ECRA. And so ultimately a decision will be made after all the information is considered. But I think sometimes it's important to ensure that the data that is presented is robust and adequately reviewed.

With that, I'm happy to answer questions. And thank you, again, for inviting me.

PREPARED STATEMENT OF GIOVANNA M. CINELLI, FELLOW, NATIONAL SECURITY INSTITUTE AT GEORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL

Panel III: Assessing Export Controls and Foreign Investment Review

Giovanna M. Cinelli
Fellow, National Security Institute
George Mason University Antonin Scalia Law School

Vice Chairman Cleveland, Commissioner Glas, Chairman Bartholomew and distinguished Commissioners, thank you for the opportunity to share with you today my perspective regarding US export controls and the foreign investment review process. It is an honor to share the podium with my colleagues, David Hanke and Kevin Wolf, each of whom brings valued insights to the issues the Commission is reviewing.

As a practitioner for over 35 years, as well as a former US Naval Reserve Intelligence Officer, I have had the opportunity to engage with several Administrations on export control and foreign direct investment ("FDI") issues before the Departments of Defense, State, Commerce, Energy, and Treasury, as well as the intelligence communities. I have participated in various export reform efforts through my appointments to a number of federal advisory committees and have seen first-hand the impact of reforms such as the DTSI initiatives under the Clinton Administration and the export control reform efforts under the Obama Administration on regulated parties. This engagement has provided me insight into practical and regulatory challenges that impact the Executive branch's ability to meet national security objectives as well as the information gaps that affect Congressional legislative proposals. Nowhere are these gaps more evident than in the changing nature of export controls and FDI.

Before providing my remarks, I would like to state that I am testifying to you today in my capacity as a National Security Fellow at the George Mason University Antonin Scalia Law School, National Security Institute. The views expressed in my testimony are personal and do not reflect the views of any organization or individual other than myself. My views are also not designed to provide legal advice, but to identify areas where legal and regulatory gaps may exist which would benefit from further study by the Commission and/or additional legislation.

Based on my experience, I address two specific areas in my testimony:

- Current vulnerabilities and risks that remain in the US foreign investment review system; and
- Recommendations for Congress based on my assessment of these issues.

These broad and complex issues affect not only the US-China relationship, but all countries and parties that are subject to the requirements of these laws and regulations or that have developed regimes that mirror the objectives of the processes the US utilizes to manage both export control decisions and FDI resolutions. As such, although the observations discussed in my testimony apply to China, they also extend to other countries and parties that are similarly situated.

It is important to lay the foundation for how the export control and FDI laws were developed and function today. This baseline provides context for my observations as well as the recommendations proposed for further Commission study and potential legislative solutions.

My observations are underpinned by five structural concepts:

- National security is not a one-size-fits-all determination. Situations exist where analyses by two or three agencies under different laws will result in inconsistent decisions. But the open-ended nature of the term, national security, is essential to the US Government's ability to flexibly manage changed circumstances and pivot more seamlessly when needed. This concept is crucial to the understanding of how export and FDI laws align and vary.

- Current export controls and FDI laws are based on a "catch and release" philosophy that broadly identifies controlled items or activities and then establishes exceptions to those controls. Starting in the 1990s, the US Government shifted its export licensing approach from one designed to "deny and delay" foreign parties from receiving US technology and products to one premised on a "run faster" concept – in essence, the US could afford to allow exports of certain levels of technology or product because US industry would maintain a several generations lead in development. This shift accommodated the growing global research and development ("R&D") environment, the desire to access the Chinese market, and transfer of primary R&D efforts from the US government to industry.

  At the same time, however, budgets for government R&D declined and industry research moved away from traditional areas of interest or relevance to US Government national security requirements. During this period, the Department of Commerce began expanding export opportunities by eliminating license requirements in favor of the use of license exceptions and changing the technical performance characteristics for items on the Commerce Control List ("CCL") to result in more technologies and products being classified in a basket category known as EAR99.

  That process continues today as demonstrated by **Attachment 1**, which includes a chart of the published export classifications conducted by the Department of State ("State") between 2010 and December 2020[1]. Of the classifications published by State, approximately 84% resulted in Commerce controlled designations. Within that 84%, approximately 26% of the products and technology (including software) were classified as EAR99. To demonstrate the impact of this

[1] These classifications represent only those that were submitted to State for review and determination. Companies complete thousands of self-classifications through internal processes which are not necessarily known to US Government policymakers. Thus, the percentages of EAR99 classifications reflected in State's database likely underrepresent the actual number of EAR99 classifications overall.

shift on the visibility the US Government and industry has into what is being transferred to foreign parties, the table below includes select examples that highlight the breadth of products that fall into this basket category.

Table 1

ITEM	CLASSIFICATION
Software that gathers information from a variety of sensors to provide situational awareness of moving objects such as manned aircraft, UAVs, birds and cars	EAR99
Master's Thesis titled "A Distributed Avionics Software Platform for Liquid-Fueled Rocket"	EAR99
A tablet developed for use in a man-portable system for neutralizing chemical agents	EAR99
An inspection system that is designed for internal robotic infrastructure inspections	EAR99
A preloaded EPROM chip with software that monitors commercial APU's operation and detects faults	EAR99
Middleware that allows customers to import and load OpenFlight 3D models and geospatial terrain databases into the Unity Game Engine	EAR99
A computer program that allows hobbyists to design a rocket and then simulate its flight	EAR99
Image generation system for civil and military aircraft simulator trainers and certain associated training and configuration-related services	EAR99
Software that provides a visual simulation of thermal infrared phenomena for aircraft operation training	EAR99
A 99.95% pure tantalum[2] plate	EAR99
Software tool designed to convert vulnerability scanner output files into a consolidated Excel workbook	EAR99

[2] Tantalum is currently listed on the US Critical Minerals List developed pursuant to Executive Order 13817 ("A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals")(December 20 2017) and Secretarial Order No. 3359 ("Critical Mineral Independence and Security") published on December 17, 2017 by the Department of the Interior. *See* CRS Report R45810, "Critical Minerals and U.S. Public Policy" by Marc Humphries (June 28, 2019), at pp. 2 and 40-43. Given this designation, tantalum provides an interesting example of how export national security determinations may conflict with other laws defining national security objectives. From an export control perspective, even with Department of Defense input into the classification, exporting agencies concluded that a tantalum product was properly categorized as EAR99 – a designation which qualifies for the least level of licensing under the EAR. At the same time, the Departments of the Interior and Defense identified tantalum and its supply as critical – both as a critical mineral and one which includes supply chain vulnerabilities. *Id*. The export laws place little limitation on the export of tantalum products, while at the same time other agencies (and even the same agency, as with Defense) view such minerals and products as crucial to various national security missions.

An EAR99 classification provides no details about a product's or technology's technical performance characteristics, its civil or military application or whether the item can be modified. Thus, even with succinct descriptions, such as those noted in Table 1, parties are not necessarily on notice regarding the potential impact to national security of the export or transfer of the item so classified.

In addition, the majority of EAR99 classified items are generally subject to license exceptions or may be exported under authorization, "No License Required," which means that there is no requirement to obtain any advanced, written permissions from the Department of Commerce. License exceptions in the Export Administration Regulations ("EAR"), which currently number 17[3], are preauthorized approvals which permit an exporter or purchaser to determine whether its proposed transfer meets the requirements for use of the exception. This licensing determination does not require confirmation by any Government agency.

While records must be maintained of transfers that occur, absent an agency request, the transfers remain unknown to US Government regulators and policy makers. This is particularly true of technology or software transfers which do not traditionally pass through the standard US Customs process. This results in visibility gaps which can impact the manner in which export regulations are drafted and/or actual license decisions occur.

- These laws have been and remain reactive. Historically, Congress and the Executive branch have managed, updated and adjusted export and FDI laws/regulations to address specific situations. Export controls trace their roots to the founding of the United States and legislation from the 1950s and the 1970s, respectively, and form the primary foundation for the current Arms Export Control Act (AECA) and the Export Control Reform Act of 2018 (ECRA).

  FDI reviews were first formalized in the Executive branch in 1975, through an Executive Order issued by then-President Gerald Ford. From 1975 to 1988, the Executive Order process functioned as expected until semiconductor production became a concern. In the late 1980s, Congress and the Executive branch noted that Japanese investors were purchasing semiconductor companies and assets to the point where supply chain and industrial base issues became pressing. This resulted in the 1988 passage of the Exon-Florio Amendments ("Exon-Florio") to the Defense Production Act ("DPA") and the beginning of the more formalized legislative underpinnings of the FDI process through the Committee on Foreign Investment in the United States ("CFIUS"). Additional revisions occurred in 1993, through the Byrd Amendment, when concerns arose over sovereign wealth fund and foreign government investments in the US.

[3] *See* 15 CFR §§ 740.3-740.4, 740.6-740.7, and 740.9-740.21.

In 2006, we encountered the issue of critical infrastructure through Dubai Ports' investment in the management of several US ports that were already under the management of a British owner. This led to the Foreign Investment and National Security Act of 2007 ("FINSA"), which opened the door to a more intense appreciation by CFIUS for critical infrastructure and co-location issues. From 2007 through 2018, the CFIUS review process continued to function until activities related to semiconductors, supply chain and civil-military fusion (a form of dual-use policies) arose, this time with questions related to Chinese investments in the semiconductor industry. This resulted in the passage of the Foreign Investment Risk Review Modernization Act ("FIRRMA").

This brief historical overview places in context the fact that legislative and regulatory changes for both export controls and CFIUS most often occur when circumstances change. In these instances, Congress and the Executive branch conclude that new authorities are needed. While responsive to the issues at hand, this approach does not address the preventive or preemptive measures that may be needed to manage shifting priorities or concerns.

- Shifting geopolitical and geostrategic circumstances appear to dictate the flexibility needed within the legal and regulatory context. Understanding the certainty of uncertainty allows for some planning on how to manage change in the business and legal/regulatory world.[4] However, unanticipated factors or accelerated timelines can alter the landscape for operationalizing compliance. For example, while many in the 1960s predicted the advent and need for globalized supply chains and workforces, many had not yet anticipated that China would be a key player in that environment. Explosive global research and development and market opportunities contributed to a misalignment of objectives between businesses and governments. National security issues were not at the forefront of economic considerations.

  This resulted in the reactive laws and regulations discussed above – a condition that made compliance and adjustments time consuming, expensive, and, in some circumstances, ineffective.

- History demonstrates that the more successful legislative and regulatory frameworks were grounded on three pillars:

  - Visibility
  - Accountability
  - Oversight

[4] As Clausewitz stated: "Our knowledge of circumstances has increased, but our uncertainty, instead of having diminished, has only increased. The reason of this is, that we do not gain all of our experience at once, but by degrees; so our determinations continue to be assailed incessantly by fresh experience." Carl von Clausewitz, *On War,* page 36.

Unless legislators and regulators understand what is occurring, it is difficult to identify gaps, whether related to national security or economic security. Without visibility into what research is being conducted, by whom, under what conditions and for what applications, the US Government and Congress lack essential building blocks to assess what may be relevant and how what is relevant can be best managed. This can result in either overly broad or overly narrow laws and regulations since the Government and Congress are unable to divine where and how to draw lines.

Accountability is equally crucial. Accountability, however, does not mean simply knowing which agency is responsible for a decision, but understanding the more granular information related to the standards against which the decision was made, the person who made the decision and the recourse available to challenge the decision made. As Chief Judge Easterbrook of the Seventh Circuit stated in a seminal export controls criminal case, *Pulungan v. United States*: "A designation by an unnamed official, using unspecified criteria, that is put in a desk drawer, taken out only for use at a criminal trial, and immune from any evaluation by the judiciary, is the sort of tactic usually associated with totalitarian regimes." 569 F.3d 326, 329 (7th Cir. 2009). Although included in a criminal case, the concept applies equally to the general need for accountability when dealing with export controls and FDI.

Tailored and structured accountability provides the regulated parties the explanations needed to understand the requirements. This is particularly important where the cloak of confidentiality is used to limit dissemination of relevant information to the public and to Congress.

Last, oversight provides the check and balance needed to keep the laws and regulations, as well as the related interpretations, within the bounds of Constitutional and administrative process[5]. Here, Congress plays a key role to ensure that legislation remains relevant, flexible and focused on the areas of concern. With that oversight comes a requirement for the Executive branch agencies responsible for export controls and FDI to provide Congress the visibility needed to understand how legislation impacts national and economic security.

[5] The President has, at times, imposed some measure of self-discipline in the regulatory interpretation process, which helps alleviate degrees of uncertainty associated with industry decision-making. For example, Executive Orders ("EO") 13891 (Promoting the Rule of Law Through Improved Agency Guidance Documents) (October 9, 2019) and 13892 (Promoting the Rule of Law Through Transparency and Fairness in Civil Administrative Enforcement and Adjudication) (October 9, 2019) limited the Executive branch's ability to interpret regulations by fiat, rather than through established administrative or regulatory review processes. Both EOs required legal and regulatory interpretations as well as enforcement to be based on administrative processes that maximized and protected engagement with the US Government by those subject to regulation. This approach provided business and industries a higher degree of certainty when managing risk-based assessments related to unclear or inconsistent regulatory requirements. These EOs remained in place until January 20, 2021, when the Biden Administration revoked each one. *See* Executive Order 13992 (January 20, 2021), bringing the degree of uncertainty injected into the regulatory process back to pre-October 2019 times.

With this background, please find below my views on the two areas I explore in my testimony.

A. Current vulnerabilities and risks remaining in the US foreign investment review system

No legal framework is gap-free and unless laws prohibit or permit all activity, the gaps remain. Both FIRRMA and the CFIUS process made significant strides to manage the changing risks related to foreign direct investments. But any process can benefit from updates that include legislative improvements that minimize embedded vulnerabilities and risks. Even with the legislative modifications noted in the first bullet below, process vulnerabilities remain that limit some of FIRRMA's effectiveness and may be addressed through further legislative updates:

- FIRRMA confirmed existing CFIUS jurisdiction, clarified areas where jurisdiction existed but may not have been exercised frequently and expanded jurisdiction for certain minority investments.

  The legislation included some significant changes in that it provided for mandatory filings for the first time since the Committee's establishment. The law also expanded the timelines for review and emphasized additional factors of concern from a national security perspective, such as supply chain vulnerabilities, key industries, personal data, and biotechnology developments. Also new, FIRRMA added a definition for critical technologies which included emerging and foundational technologies, a definition which was tied to ECRA.

  But the underlying approach to national security reviews of FDI remained unchanged – the Committee reviews submissions to determine whether the transaction resulted in national security concerns that could not be mitigated. Treasury also continued as the CFIUS chair and coordinator of the CFIUS process as well as the sole drafter of the regulations. The overall modernization effort, however, did take cognizance of changed circumstances to address key policy objectives for both Congress and the Executive branch.

- Although individual cases may be approached differently, the Committee generally takes a static, slice-in-time analysis of FDI. This approach assesses the national security risks at the time of the review but absent a mitigation agreement, the Committee loses visibility into post-clearance activities.

- The Committee remains managed as a 'flat' organization – as noted above, Treasury chairs the Committee without additional leadership from other agencies, absent the designation of a co-lead agency. But under the regulations, Treasury also controls the designation of co-lead agencies, and thus the organization and leadership structure continue to remain 'flat.' Under § 800.230, Treasury expressly

reserves the right to designate co-lead agencies,[6] which effectively minimizes each member agency's ability to take a leading role in a transaction review, absent Treasury approval. This authority appears to have been drawn originally from the predecessor statute to FIRRMA, the Foreign Investment and National Security Act of 2007 (FINSA), § 2170(k)(5), and continued in FIRRMA.

Further inquiry into the co-lead process would help inform Congress about the manner through which interagency engagements occur and national security equities are decided. This presents two areas for potential reform which may benefit the balancing of national and economic interests: 1) CFIUS member agencies should be able to self-determine whether to act as a co-lead with Treasury, rather than permitting Treasury to control that decision; and 2) once a co-lead agency is in place, the agency remains in that position unless it chooses to withdraw from that responsibility.

- US Government strategies[7], reports[8] and think tank studies have highlighted the importance of emerging and foundational technology to US national security interests and the health of the US industrial base, as well as the risks associated with the acquisition or investment into companies developing these types of technologies.[9] In an effort to address these concerns, Congress tied the identification and control of emerging and foundational technologies to ECRA. This approach, however, suffers from at least four challenges:

    - ECRA is the underlying substantive statute for the Export Administration Regulations which means that emerging and foundational technologies are viewed as presumptively controlled under the EAR. While FIRRMA refers to ECRA § 1758 for an interagency process to take into account the views of the Departments of Defense, State, and Energy, as well as other agencies as needed, there is no published timeline or statutory processes for exigencies that may require more timely action. In addition, this process may not adequately take into account that a number of emerging and foundational technologies may more appropriately be subject to controls under other US export regimes – *e.g.*, the regulations managed by the

---

6 **§ 800.230 Lead agency.** The term *lead agency* means the Department of the Treasury and any other agency designated by the Chairperson of the Committee to have primary responsibility, on behalf of the Committee, for the specific activity for which the Chairperson designates it as a lead agency, including all or a portion of an assessment, a review, an investigation, or the negotiation or monitoring of a mitigation agreement or condition.

7 *See, e.g.,* National Strategy for Critical and Emerging Technologies (October 2020), at p. 2.

8 *See, e.g.*, CRS Report R46458, "Emerging Military Technologies: Background and Issues for Congress" (Updated November 10, 2020).

9 *See, e.g.,* Twin Pillars: Upholding National Security and National Innovation in Emerging Technologies Governance (Center for Strategic and International Studies, January 2020).

Departments of State and Energy, the Food and Drug Administration and the Drug Enforcement Agency among others. Given the importance of emerging and foundational technologies to the US Government, the national security strategy and the intelligence strategy, the timeline and process for designation under the EAR may leave the US exposed to ongoing national security vulnerabilities and risks.

- Second, the EAR generally controls products and technology on the basis of multilateral regimes, such as the Wassenaar Arrangement, the Nuclear Suppliers Group and the Australia Group. Multilateral negotiations for the identification of products or technologies to be added to control lists take time and require extensive discussion. While these negotiations occur, the technologies or products at issue remain outside the purview of any export regime and are thus open to practically unlimited transfers, thereby perpetuating the national security risks that may exist.[10]

  For example, in October 2020, the Department of Commerce published a final rule adding six emerging technologies to Commerce Control List (CCL). 85 Fed. Reg. 62583 (October 5, 2020). The Federal Register notice indicated that the additions arose from the December 2019 Wassenaar Plenary Session, an almost 10-month process from multilateral agreement to addition to the CCL. During that 10-month period, the designated technologies would not have been considered critical technologies for

---

[10] Understanding the potential for gaps, Commerce established an Export Control Classification Number ("ECCN") category, 0Y521, to use as an interim classification for products or products or technology that were either not yet subject to a specific ECCN (because none existed which could accommodate the technical or performance characteristics of the item) or did not warrant control (and thus could be classified as EAR99). *See* 77 Fed. Reg. 22191-22200 (April 13, 2012). Commerce specifically stated:

"The 0Y521 ECCN series will provide a mechanism for identifying and controlling items that warrant export controls, but that are not yet categorized on the CCL or USML, such as ***emerging technologies***. It will provide a temporary control category for such items, while the U.S. Government works to adopt a control through the relevant multilateral regime(s); to determine appropriate longer-term control over the item; or determines that the item does not warrant control."

77 Fed. Reg. at 22192. Placement in ECCN 0Y512 allowed Commerce the time to review the item to best determine the appropriate classification and subsequent licensing requirements. Detailed, publicly available information about this classification process, however, remain sparse. While the concept and general process for use of ECCN 0Y521 are included in 15 CFR § 742.6(a)(8)(iii), the regulations allows the classification to expire within one year unless the Department moves the item to another ECCN or requests an extension for one additional year. To assess whether this approach was, and remains, effective, especially for emerging technology, additional public information regarding the following questions would be helpful:

- Since the establishment of this ECCN, how many products and technologies have been placed in this category?
- How many of these products or technologies have been considered "emerging"?
- To which ECCNs were these products or technologies shifted?
- How many of these products and technologies were shifted to EAR99 classifications?

purposes of FIRRMA – a gap which meant that, absent other jurisdictional grounds for CFIUS review, investments by foreign parties involving these now critical technologies might not be subject to CFIUS review and/or would be outside of CFIUS' mandatory purview.

- Third, the national security interests for export control purposes are not the same as that associated with acquisitions or investments. Exports tend to involve the provision of product, materials, equipment, software or technology in a one-time transaction or, at times, for ongoing transactions. But the entity making the sale of or transferring the products and technology retains ownership and control of the production, development, marketing and distribution processes. The national security equities, therefore, tend to examine whether the sale may advance the capabilities of the foreign purchaser or its government. An export of controlled technology to Country X may meet national security or foreign policy objectives without issue.

  But the sale of the producer of that technology to a company from Country X now implicates not only the transfers of the technology, but the control over how the operation, design, developments, supply chain and sales occur. By tying the designation of emerging and foundational technologies as critical technologies for CFIUS review purposes to export controls, FIRRMA blurs the distinctions that underpin these analyses.

- Fourth, other authorities exist for agencies such as the Departments of Defense and Energy to identify and designate critical technologies, including emerging technology. For example, P.L. 115-232 (August 13, 2018), § 1049 (Critical Technologies List) authorized the Secretary of Defense to "establish and maintain a list of acquisition programs, technologies, manufacturing capabilities, and research areas that are critical for maintaining the national security technological advantage of the United States over foreign countries of special concern." (§ 1049(a)). The Secretary is authorized to utilize the list to inform a number of decisions including but not limited to:

  > "any interagency determinations conducted pursuant to Federal law relating to technology protection, including export licensing, deemed exports, technology transfer, and foreign direct investment" (§1049(a)(1)) and;
  >
  > "inform the Department's activities of research investment strategies… and develop innovation centers and an emerging technology industrial base." (§ 1049(a)(4))

  The question for Congress may be whether the current FIRRMA-ECRA tie constrains agencies with national security equities from identifying and managing emerging technologies directly related to a national security

mission. This may be addressed, in part, by disentangling the FIRRMA-ECRA emerging and foundational technology process and allowing all agencies that are members of the Committee to identify those technologies of interest or concern. Disentanglement, however, does not mean that Commerce's authority to designate emerging and foundational would be eliminated or circumscribed. Rather, the process would be expanded to include other agencies with existing jurisdiction who could formally provide effective input to create jurisdiction for CFIUS to review cross-border transactions that may fall through the cracks based on the EAR designation process.

- FIRRMA expressly recognized the technology transfer gaps that existed in the bankruptcy processes. Sensitive technologies held by distressed parties or debtors in the bankruptcy process have been acquired by foreign parties in the past where those asset transfers did not benefit from CFIUS review. Assuming that the sensitive technologies were export controlled and the parties obtained export authorizations for the transfer of these sensitive technologies prior to the bankruptcy transfers, the Executive branch had no visibility into the potential implications to US national security interests. While FIRRMA recognized the gap, the statute did not address the process by which engagements could occur between the courts and CFIUS. As a result, the regulations do not outline how that engagement would occur.

  The bankruptcy courts have taken a keen interest in this area as concerns exist that the court process may be used to circumvent or otherwise limit CFIUS review. Training sessions provided to the bankruptcy judges as part of their annual training has highlighted gaps in existing bankruptcy statutes that limit the courts' ability to engage directly and consistently with CFIUS through a formal process. These gaps can be remedied through amendments to the bankruptcy statutes that define the process for engagement with CFIUS.

B. Recommendations for Congress

Based on the summary above, the Commission and Congress may wish to consider the following legislative proposals:

- Amendments to the bankruptcy statute[11] to accommodate the CFIUS review authorities included in FIRRMA.

[11] These amendments can be incorporated into the bankruptcy rules, as well as other tools the court uses to manage its dockets. Currently, the Advisory Committee on Appellate, Bankruptcy, Civil, criminal and Evidence Rule has scheduled hearings on the Bankruptcy Rules for January 7 and 22, 2022. Public comments regarding proposed rule changes will be accepted between August 6, 2021 and February 16, 2022. Any legislative changes made to the courts' authorities may be able to be incorporated into the rule changes scheduled.

Amendments should authorize:

- The courts to consider national security when managing asset distributions or sales through the bankruptcy process
- The creation of an ombudsman dedicated to identifying cases where national security issues may arise
- The courts to engage directly with the Department of Defense on national security issues

- Congress should consider amending FIRRMA to disentangle FIRRMA from ECRA for the purpose of identifying emerging and critical technologies. The relatively slow pace of identifying these technologies may reflect the difficulty Commerce has encountered in striking the right balance between national security concerns and industry led innovation concerns. Disentangling FIRRMA from ECRA will open the aperture directly to more input from other agencies.

  If, however, disentanglement is not possible, then FIRRMA should include provisions that authorize other CFIUS member agencies to designate emerging and foundational technologies that formally become part of cross-border transactions subject to CFIUS review. FIRRMA notes that Treasury may identify such technologies through its review of cross-border investments, but other agencies, such as the Departments of Defense and Energy have similar authorities and national security equities which would benefit their direct and independent input. The multilateral negotiation process and associated timelines to manage critical technologies under the EAR create potentially impactful delays that reduce FIRRMA's effectiveness.

- Congress should consider Senator Cotton's proposal to designate the Department of Defense as the permanent Deputy Chair of CFIUS. As the agency with primary responsibility for national security, DOD's input would help expand the resources from which national security equities can be identified. In his report entitled, "Beat China: Targeted Decoupling and the Economic Long War" (February 2021), Senator Cotton noted: "[S]uch a change [designating Defense as a permanent Deputy Chair] would ensure that Treasury will address national security concerns brought up by Defense and other organizations on the committee..." *Id*. at page 61. This may allow for a broader consideration of national security equities shared by other CFIUS members.

- Early drafts of FIRRMA included provisions that authorized members of the Committee to draft regulations for their agencies. Those regulations could inform the parties subject to CFIUS jurisdiction of the areas of interest for each member agency. Congress should consider including a similar provision in any updates to the statute.

- Confidentiality should be more clearly defined in the statute. In instances where parties issue public press releases, summaries in public filings such as Securities

and Exchange Commission notices or otherwise authorize the release of data, CFIUS should publish the non-confidential information relating to filings that have been made. The information should be included in the CFIUS annual reports to succinctly inform parties of the parties, types of transactions, industries and mitigation measures. Up until 2008, this type of information was included in CFIUS' Annual Report.

Additional issues, which extend beyond the scope of my direct testimony but which would benefit from additional study by the Commission and eventual legislative action, may be found at **Attachment 2**. Thank you for the opportunity to share my views with the Commission. I would be pleased to answer any questions.

DB1/ 124145894.1

OPENING STATEMENT OF DAVID R. HANKE, FELLOW, NATIONAL SECURITY INSTITUTE AT GEORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL

COMMISSIONER GLAS: Thank you so much Ms. Cinelli. And for our last witness here today, we have Mr. Hanke. And then we will go into question and answer.

MR. HANKE: Vice Chairman Dr. Cleveland, hearing co-chair Commissioner Glas and all commissioners, thank you for inviting me to participate in today's hearing.
I'm honored to appear alongside two of our country's true experts in this area, Giovanna and Kevin as you examine a set of critical national and economic security issues.

And it's always a pleasure to be back here in my old stomping grounds here on Capitol Hill.

Before I start, a disclaimer. The views and opinions that I express are my own and do not represent the views of the National Security Institute or my current or past employers.

From 2007 through 2019 I worked here as a staffer for Senator John Cornyn and later the Senate Select Committee on Intelligence. Senator Cornyn was the author of Foreign Investment Risk Review Modernization Act or FIRRMA and I had the distinct honor of assisting him with the staff level drafting and shepherding of this legislation.

Today, in addition to my fellowship with NSI, I'm in a private practice of law with two main focus areas: first, regulatory matters involving the Committee on Foreign Investment in the United States, or CFIUS; and, two, policy matters involving national security, strategic technologies in U.S.-China competition.

In 2016, Senator Cornyn assigned me the task of studying CFIUS and identifying any jurisdictional gaps or shortcomings. His concern was animated by the gathering national security threat posed by China and its acquisition of technology by any means possible.

FIRRMA was enacted in August 2018 as part of the fiscal year 2019 John S. McCain National Defense Authority Act. Key partners in the effort included the Treasury Department and other CFIUS member agencies and then Congressman Robert Pittenger and Danny Heck, Senator Dianne Feinstein and countless others. IRRMA was the most sweeping overhaul of the CFIUS process in its 46-year history. And it was spurred by several important realities that I'd like to cover quickly.

First, the national security landscape had evolved and CFIUS' legacy authorities were outdated and inadequate.

Second, technologies beyond the Commerce Control list and the U.S. munitions list were becoming increasingly important.

And, third, CFIUS needed to become more efficient and it needed more resources. In terms of legislative intent, FIRRMA aimed primarily to plug two gaps in the jurisdiction of CFUIS related to technology.

The first was technology joint ventures, or JVs, based overseas, arrangements through which a foreign party could conduct a de facto acquisition of an industrial capability embodied in the U.S. business.

The central concern here was that Chinese entities were steadily acquiring important know-how related to U.S. technologies that the Commerce Department had decontrolled, such as autogenerations of semiconductors.

The second of these gaps was minority position investments, typically involving Chinese backed venture capital investors.

On the way to FIRRMA's enactment, the effort to give CFIUS jurisdiction over certain technology JVs based overseas ran into heavy opposition. As a result, that provision was stripped from FIRRMA, limiting CFIUS' jurisdiction to inbound transactions and a compromised provision was drafted and substituted in. That became Section 1758 of the Export Control Reform Act, or ECRA, which created a new export control framework for emerging and foundational technologies.

The mandate for controls on foundational technologies was specifically intended to address these technology JVs based in China. The mandate for controls on emerging technologies serves a different purpose, playing a distinct jurisdictional role for CFIUS. Unless a U.S. target company's technology meets the statutory definition of critical technology, CFIUS has no jurisdiction whatsoever over non-controlling investments in these companies. The Senate passed version of FIRRMA would have granted CFIUS the authority to decide for itself which kinds of technologies were essential to national security.

House negotiators successfully pushed to eliminate that authority and instead handed it to the Commerce Department. As a result, today CFIUS has no ability whatsoever to decide which dual-use technologies should be within its jurisdictional scope.

To assess the implementation of FIRRMA, it is most useful to look separately at the process side of CFIUS and the substantive side. On the process side, FIRRMA's goal of making CFIUS more efficient has been accomplished. The Treasury Department's portion of FIRRMA implementation was completed on time by the Trump administration. Most importantly, the permanent CFIUS regulations were carefully written and timely published. Treasury did its job.

And my written testimony provides further assessment on that. On the substantive side of FIRRMA implementation, CFIUS's new jurisdiction over non-controlling investments in the areas of sensitive personal data and critical infrastructure is in great shape.

However, on the technology side, the two gaps that Congress identified have not been closed. First, on the challenge of overseas-based JVs involving foundational technologies, implementation of this portion of Section 1758 of ECRA has stalled.

Second, on the issue of Chinese backed venture capital investments involving emerging technologies, implementation of these portions of FIRRMA and ECRA has not successfully closed the gap that Congress identified.

Unfortunately, the implementation of the emerging technology controls under Section 1758 has been fundamentally at odds with this central objective of FIRRMA.
CFIUS simply cannot fulfill its expanded national security role if it has to wait years to gain jurisdiction over deals involving the most vital technologies of the future, but that is the current state of play.

Closing the two gaps that Congress identified would require reforms. I have offered several policy recommendations in my written testimony, but for the sake of time, I will leave those for the Q&A session. Thank you very much.

PREPARED STATEMENT OF DAVID R. HANKE, FELLOW, NATIONAL SECURITY INSTITUTE AT GEORGE MASON UNIVERSITY ANTONIN SCALIA LAW SCHOOL

David R. Hanke
Visiting Fellow, National Security Institute (NSI)
at George Mason University's Antonin Scalia Law School*

Testimony before the
U.S.-China Economic and Security Review Commission

Hearing on U.S.-China Relations in 2021: Emerging Risks
Panel III: Assessing Export Controls and Foreign Investment Review

Wednesday, September 8, 2021

Chairman Bartholomew, Vice-Chairman Dr. Cleveland, hearing Co-Chair Commissioner Glas, and all Commissioners, thank you for inviting me to participate in today's hearing. I am honored to appear before this Commission as it examines some of the most critical national and economic security issues of our time. And it is always a pleasure to be back in my old stomping grounds on Capitol Hill, where I spent almost a dozen years of my career serving as a staffer.

Professional Background

From August 2007 through January 2019, I worked here in the Senate, first as a policy staffer and counsel to Sen. John Cornyn (Texas) and later as a Professional Staff Member on the Senate Select Committee on Intelligence. Senator Cornyn was the author and sponsor of the *Foreign Investment Risk Review Modernization Act (FIRRMA)*, and I had the distinct honor of working for him on the staff-level drafting and shepherding of this legislation.

I concluded my government service in January 2019 and have been in the private practice of law since then. Today, my client work is centered on two main areas. First, I advise and represent clients on regulatory matters involving foreign investment screening and the Committee on Foreign Investment in the United States (CFIUS), which includes working with both investors and target companies on various types of transactions, including mergers and acquisitions, venture capital investments, and private equity transactions. Second, I advise and represent clients on policy matters involving national security, strategic technologies, and U.S.-China competition. In addition, I am a Visiting Fellow with the National Security Institute, which affords me the chance to stay involved in policy discussions such as this one.

Today, I intend to focus my testimony mainly on foreign investment screening by CFIUS, *FIRRMA*, and closely related topics, leaving the bulk of the discussion on the finer points of export control policies and regulations to my co-panelists, who fortunately are experts in that area.

FIRRMA Origins and Context

In the fall of 2016, Senator Cornyn assigned me the task of studying the existing CFIUS process and rules and identifying any jurisdictional gaps or shortcomings, as well as recommending ways

*The views and opinions expressed in this testimony are mine only and do not represent the views of the National Security Institute, my law firm or its clients, or my former employers.

by which the overall system could be strengthened and modernized through legislation. His concern was both serious and timely, animated by the gathering national security threat posed by China and its acquisition of technology by any means possible. Sen. Cornyn's work and leadership on this initiative was groundbreaking in a number of ways, both specifically on CFIUS modernization and also more generally on evolving U.S. policy towards China. And his bipartisan effort set off a cascade of China-focused legislation on Capitol Hill.

Nearly two years after Senator Cornyn launched the *FIRRMA* initiative, this legislation was enacted as part of the *Fiscal Year 2019 John S. McCain National Defense Authorization Act (FY19 NDAA)*, proving that Congress can still drive major policy reforms with broad bipartisan support and tackle complex issues, including at the tricky intersection of national security and economics. While the executive branch did not initially embrace *FIRRMA* – either in the final months of the Obama Administration or in the first months of the Trump Administration – Senator Cornyn successfully persuaded then-Treasury Secretary Steven Mnuchin (as the CFIUS chair) and other key members of then-President Trump's cabinet to support his effort and help ensure the bill was properly balanced.

While Senator Cornyn drove the process and built a powerful bipartisan coalition of partners and supporters to get *FIRRMA* enacted, this legislation would never have become a reality without the help and support of indispensable players such as the Treasury Department and other CFIUS member agencies. Key congressional partners included then-Congressmen Robert Pittenger (North Carolina) and Denny Heck (Washington), who introduced the *FIRRMA* House companion bill and led the effort in their chamber, and Senator Dianne Feinstein (California), *FIRRMA*'s lead Democrat cosponsor in the Senate. The U.S. business community – led by the U.S. Chamber of Commerce, National Association of Manufacturers, and Information Technology Industry Council – as well as other leading business organizations also supported the final version of *FIRRMA*, in part because it was paired with the *Export Control Reform Act of 2018 (ECRA*), which I will return to shortly.

FIRRMA is widely considered to be the most sweeping overhaul of the CFIUS process in its 46-year history. The legislation was informed by hundreds of meetings and calls with stakeholders in the CFIUS process, including past and current CFIUS officials at most of the nine CFIUS member agencies, CFIUS practitioners, investor groups, U.S. companies of all sizes, foreign governments, trade associations, and think tanks. Those sessions and other research led us to several important conclusions.

First, the national security landscape had evolved, and CFIUS's legacy authorities were outdated and inadequate. China had "weaponized" investment and was using it to meet strategic government objectives. It had identified gaps in both CFIUS's jurisdiction and our export control rules and was exploiting them in order to vacuum up U.S. technology and know-how. The old CFIUS jurisdiction had been relatively narrow and, as a result, unable to address many modern-day national security threats from foreign investment. And the existing dual-use export control system had some inherent weaknesses, such as preventing the overseas transfer of U.S. know-how and keeping pace with the rapid evolution of technology.

Second, in the modern national security landscape, technologies beyond the Commerce Control List and the U.S. Munitions List were becoming increasingly important to our long-term national security. Therefore, transactions involving two particular areas needed more focus from CFIUS: (a) mature, well-understood technologies that had already been downgraded by the export control system as less sensitive, but for which the U.S. business still possessed substantial know-how with national security importance (these types of technologies were later captured in the statutory

term “foundational technologies”); and (b) cutting-edge technologies developed by startups and other small companies, which in the context of long-term national security had become just as important as large defense contractors (these types of technologies were later captured in the statutory term “emerging technologies”).

Third, driven mainly by Chinese transactions, CFIUS’s case volume had increased substantially, even before any jurisdictional expansion. CFIUS simply needed to become more efficient, and it needed more personnel and other resources.

Legislative Intent Behind *FIRRMA*

At its core, *FIRRMA* was about two things: China and technology. While CFIUS also routinely scrutinizes transactions involving other areas – such as infrastructure, data, and real estate – technology was the area in which China had been doing the greatest damage to U.S. national security in recent years. To understand legislative intent, there is no better source than the legislative history and the actual words of a bill’s author. On January 18, 2018, Senator John Cornyn described the challenge in testimony before the Senate Committee on Banking, Housing, and Urban Affairs at a hearing entitled, “CFIUS Reform: Examining the Essential Elements.” Senator Cornyn stated:

> It’s not just that China poses a threat, though, it’s that the *kind of threat* is unlike anything the U.S. has ever before faced – a powerful economy with coercive, state-driven industrial policies that distort and undermine the free market, married up with an aggressive military modernization and the intent to dominate its own region and potentially beyond. To close the technology gap with the U.S. and leap-frog ahead of us, China uses both legal and illegal means. One of these tools is investment, which China has weaponized in order to vacuum up U.S. industrial capabilities from American companies that focus on dual-use technologies. China seeks to turn our own technology and know-how against us in an effort to erase our national security advantage.

Two Main Gaps

Therefore, first and foremost, *FIRRMA* aimed to plug two gaps in the jurisdiction of CFIUS related to technology deals. The first of these gaps was technology joint ventures based overseas, primarily in China. To close this gap, the original *FIRRMA* bill, as introduced on November 8, 2017, sought to give CFIUS jurisdiction over transactions through which a foreign joint venture partner could conduct a de-facto acquisition of an industrial capability embodied in the U.S. business. With these deals, a central concern for Congress was the transfer of know-how related to technologies that the Commerce Department had de-controlled, such as older generations of semiconductors.

There was a clear inconsistency between the policies underlying CFIUS’s investment screening and the Commerce Department’s regulation of outbound flows of technology and know-how. At the January 18, 2018, hearing of the Banking Committee, Senator Cornyn explained:

> The rationale behind *FIRRMA* is simple: CFIUS should be able to review transactions that have, in effect, the same national security consequences as a traditional acquisition of a U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the “back door” something they cannot get through the “front door.” To take advantage of these gaps and circumvent CFIUS review, China pressures U.S. companies

> into business arrangements such as joint ventures, coercing them into sharing their technology and know-how, enabling Chinese companies to acquire high-tech U.S. industrial capabilities and then replicate them on Chinese soil.

To address this challenge, a narrow provision was drafted in close coordination with the Treasury Department, and the new jurisdiction would have only applied where both intellectual property and know-how related to "critical technology" (as defined elsewhere in *FIRRMA*) were transferred through a collaborative arrangement between the foreign party and the U.S. business. Some in industry – especially U.S. technology and advanced manufacturing companies with large China-based operations that encompass the sharing of technology and know-how through joint ventures or related structures – aggressively opposed this narrow construct and generated enough opposition that the entire provision had to be dropped. Instead, a compromise approach was adopted, relying entirely on the export control system to address the problem. I will explain more on that below.

The second of these gaps was minority-position investments, typically involving Chinese-backed venture capital investors. These are investments that fall short of giving investors "control" of the target company, but still afford them certain rights or access that could have national security ramifications. Some deals involving foreign-controlled private equity funds and other types of investors can also fall into this category. Again at the January 18, 2018, hearing of the Banking Committee, Senator Cornyn observed that:

> China has also been able to exploit minority-position investments in early-stage technology companies in places like Silicon Valley, California, or the "Silicon Hills" in Central Texas to gain access to intellectual property (IP), trade secrets, and key personnel. The Chinese have figured out which dual-use emerging technologies are still in the cradle, so to speak, and not yet subject to export controls.

CFIUS 2.0 and the Successful Expansion of CFIUS Jurisdiction

The vast majority of *FIRRMA*'s substantive provisions survived Senate-House conference negotiations intact, though House negotiators successfully pushed for significant changes to the text in at least one key area, which I will describe below. As enacted, *FIRRMA* expanded CFIUS jurisdiction in a highly targeted fashion. It was narrowly tailored to address situations with heightened national security risks, aiming to avoid unnecessarily chilling foreign investment.

The term "CFIUS 2.0" has been adopted by some, including then-Commander of the U.S. Pacific Command, Admiral (Ret.) Harry Harris, to refer to the modernized CFIUS process under *FIRRMA*. In CFIUS 2.0, the most important new area of CFIUS jurisdiction is the previously mentioned minority-position investments. These are non-controlling, non-passive investments ("covered investments" in the parlance of the main CFIUS regulation) involving U.S. critical technologies, U.S. critical infrastructure, or the sensitive personal data of U.S. citizens. CFIUS has jurisdiction over such investments only in certain circumstances. First, the U.S. target company has to be engaged in at least one specific activity on a list, such as producing, designing, testing, manufacturing, fabricating, or developing a "critical technology"; owning, operating, manufacturing, or servicing a certain U.S. critical infrastructure system or asset; or maintaining or collecting certain types of sensitive personal data of US citizens. Second, the investment has to feature at least one of three specific non-passive triggering rights, which include (a) access to "material nonpublic technical information" in possession of the U.S. target company; (b) membership or observer rights on the company's board of directors (or the right to appoint such

individuals); or (c) involvement (other than voting of shares) in substantive decisionmaking of the target company regarding such technology, infrastructure, or data.

CFIUS jurisdiction was expanded by *FIRRMA* in two additional ways, though these are less relevant to today's topics. These are transactions that are "designed or intended to evade or circumvent" the jurisdiction of CFIUS, and transactions involving stand-alone real estate near sensitive locations (under a separate regulation, 31 C.F.R. Part 802).

Compromises in *FIRRMA* on the Way to Enactment

As mentioned, during congressional consideration of *FIRRMA*, some U.S. companies with major business interests in China aggressively opposed the specific provision that would have given CFIUS jurisdiction over certain technology joint ventures based overseas, arguing in favor of the status-quo hands-off approach taken by the U.S. Government to date on these particular types of joint ventures. As a result, that provision was stripped from *FIRRMA*, limiting CFIUS's jurisdiction to inbound transactions only, and a compromise provision was drafted with the help of the executive branch and substituted into *FIRRMA*. Opponents of *FIRRMA*'s original construct were much more comfortable with maintaining the locus of any outbound controls and critical technology definitions at the Commerce Department, which had been generally far less concerned about technology and know-how flows to China.

On paper, Section 1758 created a new export control framework for "emerging and foundational technologies." During *FY19 NDAA* conference negotiations on *FIRRMA* and *ECRA*, this provision migrated from *FIRRMA* over to *ECRA* and was then enacted as *FY19 NDAA* Section 1758 (codified at 50 USC § 4817). This provision was intended to address some of the shortcomings that Congress had identified in the existing dual-use export control system, such as its struggle to prevent the overseas transfer of important U.S. industrial capabilities and its inability to keep pace with the rapid evolution of technology. With this provision, Congress handed the Commerce Department a statutory mandate to lead an interagency process for identifying and unilaterally controlling emerging and foundational technologies "that are essential to the national security of the United States." This provision, coupled with one in *FIRRMA*, also created stronger connective tissue between the CFIUS and export control processes. CFIUS's previous regulatory definition of "critical technologies" already included the U.S. Munitions List and key portions of the Commerce Control List. *FIRRMA* expanded this definition by adding the concept of "emerging and foundational technologies." The provision requires unilateral controls initially for each technology, limited to a three-year period during which BIS must pursue multilateral controls for that technology.

The mandate for controls on foundational technologies was specifically intended to address the national security concerns regarding technology joint ventures based in China, such as those in the field of semiconductors, through which important U.S. industrial capabilities were being steadily acquired by Chinese entities. The authors of *FIRRMA* had originally intended for CFIUS to regulate these de-facto acquisitions of industrial capabilities, but instead the job would now remain with the export control system under the mandate of Section 1758.

Although the mandate for controls on emerging technologies is intertwined with the mandate on foundational technologies, it serves a somewhat different purpose. It was intended to play a distinct jurisdictional role for CFIUS. As mentioned above, in CFIUS 2.0, jurisdiction over non-controlling, non-passive investments in the technology sector depends explicitly on whether the U.S. target company works with a technology that meets the definition of "critical technology."

Without a critical technology, CFIUS has no jurisdiction whatsoever over these types of transactions.

When Congress expanded CFIUS jurisdiction to cover certain minority-position investments, the problem it was focused on was China's growing participation in venture capital deals involving early-stage technology companies. In January 2018, the Department of Defense's Defense Innovation Unit Experimental (DIUx) published a timely report, entitled "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," which examined this very issue. Among its findings were the following: (1) Chinese participation in venture-backed startups had grown rapidly in recent years, reaching a record level of 10-16% of all venture deals from 2015 to 2017; and (2) China was investing in key technologies such as artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, blockchain technology, and gene editing – many of which are of great interest to the U.S. military.

This eye-opening DoD analysis became one of the analytical underpinnings of the *FIRRMA* initiative. The members of Congress who drove *FIRRMA* recognized the growing national security importance of startups and other small companies and the types of technologies that they were developing, which by their very nature were "emerging" technologies. However, the proper way to determine which technologies were important or sensitive enough to warrant a CFIUS review of related investment deals was a matter of some disagreement between the Senate and the House.

The version of *FIRRMA* passed by the Senate on June 18, 2018, as part of the *FY19 NDAA* (which was identical to the version reported out by the Senate Banking Committee) would have codified in statute CFIUS's then-existing regulatory definition of "critical technologies." However, importantly, it would also have created a new prong of "critical technologies" with jurisdictional implications for CFIUS. Under this expanded definition, CFIUS would have been granted the authority to decide for itself, as an interagency committee, which kinds of "technology, components, or technology items" were "essential to national security" and thus might warrant CFIUS review of a related investment, beyond those technologies that already met the definition of critical technology per controls issued by the Commerce Department or State Department, for example.

As referenced above, during Senate-House conference negotiations, there was a burst of last-minute lobbying from companies aiming to expand their operations in and sharing of technology and know-how with China. This succeeded in pressuring House negotiators into taking the position that the key function of determining a particular technology's sensitivity or importance should remain beyond the reach of CFIUS. House negotiators successfully pushed to eliminate that authority for CFIUS and to instead hand unilateral authority to the Commerce Department to decide what additional dual-use technologies might be "essential to the national security of the United States" (as outlined above) and thus appropriate for CFIUS to prioritize in its investment screening role. As a result of that 11th-hour change to *FIRRMA*, today CFIUS has no ability whatsoever, as an interagency committee, to decide which technologies should be labeled "critical technologies" for the purpose of setting the proper scope of its own jurisdiction.

Assessing *FIRRMA* Implementation To Date – Process and Substance

Of course, no legislation is perfect – and *FIRRMA* is no exception – but even a very good piece of legislation must be properly implemented by the executive branch in order to meet

congressional intent. To assess the implementation of *FIRRMA*, it is most useful to look separately at what was done on the process side of CFIUS and what was done substantively.

Assessing the Process

On process, the Treasury Department was always the key player in *FIRRMA* implementation and, thankfully, its portion of implementation was completed on time prior to the end of the Trump Administration. There is a lot to celebrate in *FIRRMA*'s implementation on the process side of things. For example, Treasury launched the "Critical Technology Pilot Program" within 60 days of *FIRRMA*'s enactment, which was impressive speed, especially by government standards. More importantly, the permanent CFIUS regulations under 31 C.F.R. Part 800 and 31 C.F.R. Part 802 were thoughtful, carefully written, closely tailored to the problem set, and timely published. CFIUS did an admirable job of maximizing certainty and predictability for transaction parties wherever possible.

Of course, one of the central goals of *FIRRMA* was to make the CFIUS process more efficient. That necessitated, among other things, providing CFIUS with an overdue boost in resources to hire additional personnel and improve its infrastructure to prepare for a heavier workload per the jurisdictional expansion. That boost was funded in part by successful implementation of new authority for CFIUS to collect filing fees, which *FIRRMA* had granted. Among the additional personnel hired by CFIUS was the group referred to in a January 2021 *Wall Street Journal* article as a "buzzy SWAT team," whose mission is to identify transactions that were never filed for CFIUS review but nonetheless could pose a national security risk. That important work had been mandated by *FIRRMA* in *FY19 NDAA* Section 1710, which required CFIUS to establish a process for identifying these "non-notified and non-declared" deals.

FIRRMA's greatest process improvement was arguably the creation of a new short-form CFIUS filing called a "declaration," which is a streamlined, five-page filing that depending on the situation can be either mandatory or voluntary (for more benign transactions). In early drafts of *FIRRMA*, these short-form filings were strictly voluntary, intended to give parties an option for fast-track review and potential CFIUS clearance. Later, the concept of mandating declarations in certain situations was proposed and incorporated into the legislation. Treasury's implementation of the declaration concept has been excellent, and the use of these filings is already expanding as transaction parties and CFIUS practitioners gain a better understanding of where declarations are most appropriate and useful.

On mandatory declarations, the CFIUS member agencies (including the Commerce Department and the State Department, the key agencies on export controls) worked together to craft a clear rule, which was issued on September 15, 2020. The new rule ties CFIUS mandatory filing requirements to the question of whether a U.S. Government export license or other authorization would hypothetically be required to transfer the U.S. target company's critical technology to either the relevant foreign investor or parties holding significant interest in the foreign investor.

Treasury also utilized *FIRRMA*'s "country specification" authority (in *FY19 NDAA* Section 1703) to create a positive list of "excepted foreign states," allowing "excepted investors" from those nations to self-classify as meeting the full requirements to be exempt from two of the new areas of CFIUS jurisdiction. While only three nations – the United Kingdom, Canada, and Australia – qualify at the moment, the list is likely to be broadened in the coming years to include additional allied nations and narrow the pool of covered transactions, allowing CFIUS to deprioritize benign transactions. The employment of this list also has the effect of creating an important incentive for

foreign countries to set up or enhance their own foreign investment screening process, an important development that I will discuss in more detail below.

Additional efficiencies in the CFIUS review process have come as a result of the fact that, in *FIRRMA*, Congress lengthened the review period (the initial phase of the CFIUS process) by 15 days, making it 45 days instead of the previous 30 days. This has allowed CFIUS to complete more reviews during this first phase, without needing to cross into the second 45-day period (the investigation). It has also reduced the pressure on transaction parties to potentially have to withdraw and refile with CFIUS to restart "the clock" during more complex reviews.

One of the most important effects of *FIRRMA* stems from the provision in *FY19 NDAA* Sec. 1713 on establishment of a formal process for CFIUS engagement with allied and partner nations, intended to "facilitate the harmonization of action with respect to trends in investment and technology," provide for information-sharing regarding "specific technologies and entities acquiring such technologies," and "include consultations and meetings with representatives of the governments of such countries on a recurring basis." The Treasury Department took this task seriously and dedicated the time and energy necessary to get it right. In July, Tom Feddo, the former Treasury Assistant Secretary who oversaw the CFIUS process for the Trump Administration, posted some insightful statistics on this:

> With *FIRRMA*'s enactment Treasury expanded its CFIUS staff over five-fold and assembled a team dedicated to building international relationships and cooperation. It collaborated at length with the Five Eyes, Japan, and the EU, and by mid-2020, Treasury had engaged with "the G7 Finance Ministers, Australia, Canada, and the United Kingdom," "interacted over 260 times with nearly 50 counterpart countries or multilateral entities," and was leveraging "the rising tide of growing global interest in establishing and reforming investment review regimes." Treasury advised several allies on these reforms, and emphasized to others the critical need to establish mechanisms to protect cutting-edge technology from misappropriation.

Since *FIRRMA*'s enactment, many U.S. allies and partner nations have taken major steps to create or expand their own inbound investment screening mechanisms, and this is one of the most important legacies of *FIRRMA*. Making the screening of foreign investment more consistent across allied and partner nations not only more effectively addresses the potential risks to the national security of the United States and our allies and partners; it also helps maintain a more level playing field for companies whose global competitors might otherwise benefit from a proposed investment that is problematic from a national security standpoint.

The Biden Administration is continuing CFIUS's important multilateral engagement as the new E.U.-U.S. Trade and Technology Council gets off the ground, with cooperation in investment screening reportedly a major theme of the upcoming meeting.

Assessing the Substance

On the substantive side of *FIRRMA* implementation, the good news is that CFIUS's new jurisdiction over "non-controlling investments" in the areas of sensitive personal data and critical infrastructure is in great shape. The regulations did a fine job of employing CFIUS's newfound authority and addressing the national security risks, while also drawing clear lines for transaction parties.

However, on the technology-centric areas of CFIUS's expanded jurisdiction and the Commerce Department's mandate to control emerging and foundational technologies under Section 1758, the question must be asked as to whether the relevant U.S. Government agencies have closed the two gaps that Congress identified, implementing *FIRRMA* and *ECRA* as envisioned by Congress. First, on the challenge of overseas-based joint ventures involving foundational technologies and the transfer of related know-how, implementation of this portion of *ECRA* never got off the ground during the Trump Administration and unfortunately appears to remain stalled in the Biden Administration. Second, on the issue of Chinese-backed venture capital investments involving emerging technologies, implementation of these portions of *FIRRMA* and *ECRA* has not successfully closed the gap that Congress identified. Unfortunately, the last-minute changes that were made during the Senate-House conference negotiations in an attempt to water down *FIRRMA* have made CFIUS totally dependent on the Commerce Department to determine CFIUS's jurisdiction over these types of transactions, as explained above.

The Commerce Department's process for identifying and controlling emerging and foundational technologies has been highly deliberative, with a great deal of input having been solicited from and provided by industry and academia, including through the notice-and-comment process. It has also been incredibly slow. With both emerging technologies and foundational technologies, the Commerce Department is taking a two-step process: issue an Advance Notice of Proposed Rulemaking (ANPRM), then publish individual controls as they become ready (not all of them simultaneously). As Section 1758 requires, it will be an "ongoing" process, not a one-time exercise.

On foundational technologies, the Commerce Department published an ANPRM on August 27, 2020, soliciting public comment on potential approaches for identifying these technologies. It received several dozen public comments from industry and academia, but it has yet to impose any foundational technology controls or announce additional steps being taken to meet its mandate.

On emerging technologies, the Commerce Department issued an ANPRM on November 19, 2018, asking for input on how to identify and control these technologies. It listed 14 broad categories of "representational technologies" to give commenters some idea of what was under consideration. Over 200 comments were submitted to the Commerce Department. Since then, the Commerce Department appears to have issued one unilateral emerging technology control last January on "software specially designed to automate the analysis of geospatial imagery." In addition, according to its 2020 annual report, the Commerce Department has imposed controls on 36 other emerging technologies pursuant to *ECRA*, most of them multilateral controls through the Wassenaar process or the Australia Group.

In the export control context, multilateral and plurilateral controls are certainly preferable to unilateral controls in most ways, especially because they help maintain a level playing field for U.S. companies. However, multilateral controls suffer from one major disadvantage as compared to unilateral controls, and that is the amount of time it can take to impose them. In the investment screening context, relying on slow-moving multilateral controls to determine the jurisdiction of CFIUS over non-controlling, non-passive investments is highly problematic given the consensus nature and lumbering pace of action in organizations like the 42-member-country Wassenaar Arrangement. One must keep in mind that it can take two to three years, from start to finish, to actually impose a multilateral control through Wassenaar. In contrast, the technologies being developed by dynamic U.S. startups typically move and change much more rapidly than that, and venture capital investments (including those involving foreign investors) in these companies often happen quite quickly.

Unfortunately, the implementation of the emerging technology controls under Section 1758 has been fundamentally incompatible with a central task that Congress assigned to CFIUS when it enacted *FIRRMA*, namely to address Chinese-backed venture capital investments involving emerging technologies. CFIUS simply cannot fulfill its expanded national security role in the new era of strategic competition if it has to wait years to gain jurisdiction over foreign investments in U.S. companies that are developing the most vital technologies of the future. Relying on Wassenaar to help determine the jurisdiction of CFIUS is a major policy mistake, but that is the current state of play with the implementation of emerging technology controls under *FIRRMA*.

As things stand, for example, a state-owned enterprise (SOE) from a foreign adversary nation (e.g., China or Russia) could invest in a U.S. company that is successfully developing leading-edge quantum computing or machine learning technology in a place like Silicon Valley. The SOE could take a 10% voting interest in the company, a seat on its board of directors, and potentially other significant investor rights – and CFIUS would have no ability to even review the deal, so long as the U.S. Government has not yet imposed export controls on that specific technology. (Of course, regarding the foreign investor, entities that are subject to blocking sanctions by Treasury's Office of Foreign Assets Control would have restrictions.) This is a worst-case scenario that may be unlikely, yet it illustrates what is currently possible. The implications for U.S. national security are significant, and there are better ways to make technology determinations for the purpose of setting the proper scope of jurisdiction for CFIUS.

As this Commission noted in its June 1, 2021, report, "Unfinished Business: Export Control and Foreign Investment Reforms," authored by Policy Analyst Emma Rafaelof:

> Defining a list of "emerging and foundational" technologies is a crucial part of implementing the *Foreign Investment Risk Review Modernization Act (FIRRMA)* and the *Export Control Reform Act (ECRA).* Since these acts became law in 2018, there has been a significant delay in forming this list along with a lack of clarity on the process and methodology.
> . . .
> Lack of clarity from the Department of Commerce on what constitutes emerging and foundational technologies impedes the ability of the Committee on Foreign Investment in the United States (CFIUS) to fulfill its responsibilities. The years-long delay in developing these definitions may exacerbate national security risks.

A January 15, 2021, report by Ian Fergusson and Karen Sutter of the Congressional Research Service, entitled "U.S. Export Control Reforms and China: Issues for Congress," echoes these conclusions:

> The lack of new technology identification arguably impedes not only *ECRA* implementation but also congressional reforms that expanded the authority of the Committee on Foreign Investment in the United States (CFIUS) to review Chinese and other foreign investments in critical and emerging technologies below a traditional threshold of foreign control. CFIUS can only act against non-controlling foreign investments if the technologies involved in the transaction are controlled.

CFIUS, through no fault of its own, has likely been unable to review a single non-controlling, non-passive investment involving emerging or foundational technologies controlled under Section 1758 during the three years since Congress expanded CFIUS's jurisdiction through *FIRRMA*. Today, most venture capital deals in the technology space likely remain beyond the reach of CFIUS, typically because the technology does not meet the definition of "critical technology."

While the issuance of lists of emerging technologies and foundational technologies was what the congressional authors of *FIRRMA* envisioned, the Commerce Department has made clear that it does not plan to do that. Instead, it intends to issue very narrow, precise controls on specific items, software, and technologies, just as it does under the legacy export control system. Unfortunately, *FIRRMA* can never have its true intended effect until either the process for controlling emerging technologies and foundational technologies is carried out as Congress envisioned or Congress enacts a better approach.

Implementation Status for Other Provisions of *ECRA*

Beyond its CFIUS implications, *ECRA* itself is a solid piece of legislation, but more than three years after its enactment the implementation status for other parts of it remains in question. One example is *FY19 NDAA* Section 1759 (codified at 50 USC § 4818), which requires the Commerce Department to work jointly with the Departments of Defense, State, and Energy to conduct a review of license requirements for exports, reexports, or in-country transfers of items to China and other arms-embargoed countries. The deadline for compliance was May 2019.

It is also unclear whether an important *ECRA* provision that aimed to improve congressional oversight of the export licensing process has been implemented. In *FY19 NDAA* Section 1761, subparagraph (h) contains the following requirement:

> Any information obtained at any time under any provision of the Export Administration Act of 1979 (50 U.S.C. 4601 et seq.) (as in effect on the day before the date of the enactment of this Act and as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)), the Export Administration Regulations, or under this part, including any report or license application required under any such provision, shall be made available to a committee or subcommittee of Congress of appropriate jurisdiction, upon the request of the chairman or ranking minority member of such committee or subcommittee.

The scope and scale of dual-use technology transfer to China that has occurred over the past two decades (both voluntarily and involuntarily) is staggering, but Congress has very limited visibility into the relevant export licensing decisions. Improving transparency in this area would enable better congressional oversight. It would also better equip any administration to draw lines at the appropriate places to protect U.S. competitiveness and innovation. If the U.S. Government does not have detailed information on the technology and know-how that is leaving our shores for China, it will invariably draw lines in the wrong place when it comes to regulating such flows.

Congress already conducts this type of oversight in the CFIUS process and other areas of export controls. For example, after CFIUS case decisions, notification is required by statute to be sent to Congress, which often takes advantage of the opportunity to receive briefings from CFIUS on the details of the transaction and its disposition. Similarly, for export control licensing decisions that fall under the purview of the State Department, my understanding is that State has a regular process of briefing its congressional oversight committees. Congress may wish to establish a similar process and flow of information with the Commerce Department.

Policy Recommendations

Tinkering with *FIRRMA*

Closing the two gaps that Congress identified at the outset of *FIRRMA*'s development would likely require both legislative and administrative reforms. With Section 1758, Congress created a flawed construct for the identification and control of emerging and foundational technologies, though both Congress and the Commerce Department have an opportunity to take meaningful steps to remedy the problem. Unlike when Congress enacted *FIRRMA* and *ECRA*, sweeping changes to the process are not required. Instead, some targeted "tinkering" with the current rules would go a long way, though many stakeholders would certainly be leery of the idea of revisiting CFIUS reform just three years after *FIRRMA*.

On the challenge of non-controlling, non-passive investments involving emerging technologies, legislation would likely be required to repair the broken mechanism that is currently used to define the jurisdiction of CFIUS in this area. The cleanest and simplest approach may be to loosen the jurisdictional linkage between *FIRRMA* and *ECRA* in this area, reverting to an approach similar to the one taken in an earlier version of *FIRRMA* that was passed by the Senate as part of the *FY19 NDAA*, as described above. That would give CFIUS the flexibility to decide for itself – as a powerful cabinet-level interagency committee with deep expertise in the full spectrum of national security issues – which technologies beyond the existing list of critical technologies are indeed essential to national security and thus might warrant CFIUS review of a related investment. CFIUS could use that authority to create and employ categories of technology for jurisdictional purposes, in a way that is much more useful and relevant than relying on ultra-narrow export controls buried in the nooks and crannies of the Commerce Control List.

There are compelling reasons to revisit these particular aspects of *FIRRMA* and *ECRA*. Many of the potential national security risks involved in CFIUS's screening of non-controlling, non-passive foreign investments in U.S. target companies are uniquely different from the risks that the export control rules aim to address. In considering whether to allow a specific foreign entity to invest in a particular U.S. company, CFIUS has to worry about the likelihood of the foreign party gaining less tangible things, such as insights into the company, its business practices, its past experience with and future plans for research and development, and its overall sector; connections with key company personnel and important suppliers, partners, and customers; and leverage regarding the company and the direction of its future technology pursuits. These present questions related more closely to economic espionage than to technology transfer, for example. On the investment screening side, there are a set of risks that are simply different from those on the export control side.

Members of Congress are already proposing reforms to Section 1758 and the CFIUS definition of critical technologies. Senator Thom Tillis (North Carolina) introduced legislation last year that would make a targeted change to authorize the Treasury Department (as chair of CFIUS) to designate emerging and foundational technology for CFIUS-only purposes (with no export control implications whatsoever), but only if one other voting member of CFIUS agreed.

The House Republican China Task Force report from September 2020 has likewise weighed in on the importance of full implementation of the Section 1758 mandate and has recommended looking at transferring the function to a different agency altogether: "If DoC's Bureau of Industry and Security is unable to make substantial and measurable progress in fulfilling this requirement, Congress should consider whether a different bureau or department can better fulfill this statutory obligation."

On the specific challenge of overseas-based joint ventures involving foundational technologies and the transfer of related know-how, the gap could still be closed by the Commerce Department administratively without the need for legislation action. The coming months may bring important developments in this area. However, there is mounting frustration on Capitol Hill about this particular issue, as well as on much broader ones involving China's desire to dominate and leverage global supply chains in areas such as personal protective equipment and pharmaceuticals.

New Proposals to Screen Outbound Investments

The National Critical Capabilities Defense Act, bipartisan legislation authored by Senators Bob Casey (Pennsylvania) and John Cornyn (Texas), is under active consideration now on Capitol Hill and with certain improvements would be an appropriate reform. This bill would create an interagency federal process, led by the U.S. Trade Representative (USTR), to screen outbound U.S. investments and the "offshoring of critical capacities and supply chains to foreign adversaries, like China and Russia . . . ."

The Biden Administration, at very senior levels, is also thinking about this set of problems and has expressed concern. President Biden's National Security Advisor Jake Sullivan recently said

> And then of course we have to work closely and especially closely with our partners on our export control and investment screening regimes to make sure they are postured for intense technology competition. In this regard, we are also looking at the impact of outbound U.S. investment flows that could circumvent the spirit of export controls or otherwise enhance the technological capacity of our competitors in ways that harm our national security.

Other executive-branch developments in the area of overseas-based joint ventures, potentially involving foundational technologies, are also worth noting. Recently, the White House and the USTR announced cooperative frameworks with both the European Union and the United Kingdom pertaining to civil aircraft. The Biden Administration is apparently working with both of them on "common approaches and enhanced cooperation regarding the screening of new outward investments in joint ventures and production facilities in non-market economies."

There seems to be an increasing alignment of interests and objectives between key members of Congress and key players in the Biden Administration in tackling this issue. As such, this may present a unique opportunity to build a carefully calibrated new interagency process, with the Casey-Cornyn legislation as the jumping-off point, setting the bar in the right place on the screening of outbound investments and technology flows. To strike the right balance, the private sector must be part of the thought process and willing to provide Congress and the Biden Administration with substantial input, as occurred during the development of *FIRRMA* and *ECRA*.

Other Potential Improvements to CFIUS

With CFIUS, the challenge remains how to properly address national security risks without overloading the process and "breaking" it. Of course, not all transactions present real national security risks, and therefore not all warrant the same level of scrutiny and commitment of CFIUS's time and resources. Focusing the work of CFIUS on transactions with actual national security risks, versus benign transactions, is the key. A particularly effective way to conduct this triage function would be to further differentiate deals based on a foreign investor's home country.

One option would be for CFIUS to tighten the focus of its reviews by employing a negative list of "foreign adversary" countries, much the same way the Commerce Department did with its January 19, 2021, rule on "Securing the Information and Communications Technology and Services Supply Chain." This rule established a screening process for ICTS transactions, focusing only on five specific "foreign adversaries" (China, Russia, Iran, North Korea, and the Maduro regime in Venezuela). CFIUS could certainly emulate such an approach in administratively re-scoping its jurisdiction, where appropriate. In fact, early drafts of *FIRRMA* had proposed utilizing this type of negative list of higher-risk countries to cabin the new areas of CFIUS jurisdiction. At the time, this proposed approach was rejected by the executive branch, though it received strong support from the House and from many key players in industry, including the U.S. Chamber of Commerce. Moreover, the previously mentioned "country specification" authority provided by *FIRRMA* is very broad, and could arguably be employed for this very purpose.

CFIUS remains a largely voluntary process, and that should continue to be the case. Mandatory filing requirements should be highly targeted and put in place only where truly necessary, because the filing of either full-length CFIUS notices or short-form CFIUS declarations necessitates CFIUS spending time and resources scrutinizing the transaction in response. However, creating a new, purely informational ultra-light filing (perhaps called a CFIUS "disclosure") could be a value-added tool for CFIUS. In the paper age, such a filing might have been referred to as a "postcard" filing. Today, it could be a very basic online filing that imposes only a minimal burden on transaction parties. It could be used by CFIUS to gain more visibility into deals that otherwise have no mandatory declaration requirement, but have a discernable nexus to a foreign adversary nation and involve specific sectors and areas that are of high priority to that nation, such as "Made in China 2025," China's Five-Year Plans, and other industrial policy.

In general, congressional oversight hearings on the implementation of *FIRRMA* and *ECRA* are long overdue. With implementation still incomplete, the onus is on Congress to assess the causal factors and decide on appropriate actions. Additionally, as CFIUS assesses national security risks on transactions in the pandemic era, Congress should ensure the process is taking into account the overall market share of the U.S. target company's general technology that is already held by any foreign country that is involved with the transaction.

Miscellaneous Reforms

Recently, Congress has also been considering reforms regarding the "Operating Committee," a key part of the interagency dispute resolution process for export licensing decisions. An amendment on this was recently proposed by Congresswoman Claudia Tenney (NY-22) during a markup of the House Foreign Affairs Committee, but it was voted down. The concern from some in Congress has been that, at the Operating Committee, the Commerce Department has the authority to overrule national security concerns raised by the other members – the Departments of Defense, State, and Energy – and grant an export license anyway. This may be a fruitful area for oversight and reform.

Lastly, the U.S. Government needs to improve its toolkit for helping worthy U.S. target companies that may find themselves in the crosshairs of CFIUS and end up having a transaction blocked or a divestment forced. Unfortunately, these companies sometimes have no other available sources of capital for the purpose of competing, expanding, scaling up, pursuing new technologies and product lines, and generally succeeding in the marketplace. It is in the U.S. national security and economic interest to ensure that these types of companies still exist and are thriving five or 10 years from now, and that will necessitate some new and creative approaches. Merely telling companies to avoid Chinese investment and hoping that private investors will save the day is not

going to be an adequate long-term policy in the era of strategic competition. In 2021 and beyond, a strong defense (i.e., CFIUS) must be paired with a good offense – some active mechanism for helping certain companies secure private capital or some type of short-term government support. Of course, the Senate recently passed the *U.S. Innovation and Competition Act (USICA)*, which takes some steps to provide alternative sources of funding, and the House has passed related legislation. This is a decent start, although *USICA*'s initial focus on technology has already been watered down and seems likely to get further diluted as the Senate and the House negotiate over a final version of the legislation. To get these policies right, more congressional attention will likely be needed in the near future.

COMMISSIONER GLAS: Thank you so much, Mr. Hanke. I am going to defer to our vice chairwoman, Robin Cleveland, who's been so gracious today, to help with the question and answer since she is physically in the room with some of the participants. So, Robin?

VICE CHAIRMAN CLEVELAND: Thank you. I can actually just see people. So I think we are going to go in reverse alphabetical order, so we'll start with Commissioner Wong.

COMMISSIONER WONG: Mr. Hanke, thank you for testimony. Just at the end there you talked about the gap related to joint ventures, you know, being able to execute de facto acquisitions of critical technology, that that gap has not been filled despite the legislative intent. Could you just quickly explain why that gap hasn't been filled? What was the delay?

MR. HANKE: Well I think our previous witness is probably better situated to explain why the reason for the 37-month delay since Congress has enacted that statute. I'm talking about ECRA here.

But I think the, you know, it's a challenge, you know, the challenge of identifying and controlling foundational technologies is difficult.

There are no new authorities, no new budget that comes with Section 1758. It's purely a mandate. So no federal government agency relishes the thought to get a mandate with no bennies attached to it.

But nonetheless, the deal that was struck in the drafting of FIRRMA and ECRA was that CFIUS will not have jurisdiction over these kinds of joint ventures. That was -- there was a lot of opposition, as I said in my testimony.

Instead, this function would be punted to the export control system where it had resided for decades, in fact, where the problem had not been addressed.

And so with this new-found mandate, Congress was left to go back and revisit the problem and take a second crack at it. There's really no good reason why 37 months later not a single substantive step has been taken.

But perhaps the Commission can unearth some reality on that. I'm not sure.

COMMISSIONER WONG: I yield the rest of my time back.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Wessel, yes, you're there.

COMMISSIONER WESSEL: Yes. Thank you to each of the three witnesses. I had worked with various capacities over a long time, including Kevin as his former campaign colleague many years ago. So thank you all for being here today.

Let me first start with a question for Giovanna and David. Giovanna, my understanding is that companies go to great lengths to manage coverage under export controls in CFIUS in order to limit U.S. jurisdiction and that it's fairly easy to develop interpretations that avoid the rules. Can you comment on that issue?

MS. CINELLI: So any law and regulation -- thank you for the question. Any law or regulation that is drafted with a catch and release approach, by definition, results in opportunities to interpret the release portion of the regulation to allow for maximum flexibility.

And with that flexibility comes the ability to decide whether the law applies in your particular circumstance and, if so, under what circumstances.

So in the Export Control Reform Act, no changes were made to the Export Administration Regulations on the use of license exceptions or how licenses or policy controls

were put in place. So rules such as the de minimis or the Foreign Direct Product Rule that was discussed by Undersecretary Pelter remain in place.

And what this allows an organization or an individual to do is to assess the amount of U.S. content in a particular product, technology, software, equipment and make a determination that it falls between a specific threshold. Then it is no longer subject to those regulations. And it is fully aligned with the way the laws are currently put in place. And so the compliance organizations and companies spend time looking at their product and technology offerings to try to understand exactly what is involved in those, in the development, in the design to make an assessment as to what the U.S. content is.

This has been a challenge in some circumstances, but in others it has not. Just one point of reference, the recent attempt to implement a Software Bill of Materials, President Obama issued an executive order that established moving forward with the Software Bill of Materials.

And there have been published guidelines put out by NIST and Commerce in July of this year. If you look at the elements that are required to meet it, you can see the complexity of the problem.

But that doesn't change the nature of the regulation that says, however I define software I can decide what the amount of U.S. content is or is not in that particular product, so --

MR. HANKE: Commissioner Wessel, thanks for the question. I want to distinguish between a term that you used and maybe some other terms. You used the term, I believe, avoid. And avoid is a verb. We also have verbs like --

COMMISSIONER WESSEL: I mean manage -- manage, not avoid.

MR. HANKE: Manage. You know, I think it's important to point out that CFIUS has limited bandwidth and that Congress, in rescoping the jurisdiction of CFIUS, wanted them to focus on the actual risks and not the ones where -- not deals where there might be really very minimal or no national security risk.

And so the judgment was made that certain features, certain rights that the foreign investor would possess are associated with national security risk. And if those features are not present in the deal, then there's really very little reason to be worried about it.

And so there's really a sense of sort of desirable beneficial avoidance, lawful avoidance that you should want and that, in fact, in the drafting of FIRRMA, that we provided a bit of a road map for parties to craft deals, to structure deals in a way that CFIUS would not be concerned about national security.

Because there's things like a board seat that has been removed from the deal. Certain control rights are removed from the deal -- certain access to proprietary or technical information not present in the deal.

So when these changes are made, there's really no reason for CFIUS to be concerned -- very little reason. And so I think that's something that we should strive for.

So that's a way of addressing the problem without the government needing to jump in with both feet and do a very painful, lengthy, expensive national security review. And so I just wanted to make that distinction.

COMMISSIONER WESSEL: Thank you. On a separate issue which you had in your testimony and always appreciate the -- Senator Cornyn's desire to engage in bipartisan legislating -- is the question of outward bound investment group as one of your recommendations. How do you see that moving forward? I believe the senator has the legislation?

MR. HANKE: Right, there's a bill called the National Critical Capabilities Act -- I believe that's the full name -- by Senator Casey and Senator Cornyn. I believe it was introduced in May and I mentioned it in my testimony.

In some ways, this is sort of a Congressional revisiting of the same kind of joint venture problem, the offshoring of certain functions that would involve designing, manufacturing, owning, developing certain capabilities. Not a focus on technology but a focus on capabilities. And the twin sort of considerations of national security and emergency preparedness are what animates that bill. There's a process by which the federal government would identify those capabilities, would decide what, indeed, is important, what should trigger some kind of interagency review.

And I think that's worth doing. That's something that Congress -- the government should want to have visibility on, should one have an ability to decide whether the manufacturing of PPE is going to be moved to China, whether certain pharmaceuticals are going to be relocated offshore. These are critical questions.

So where is that headed? I believe that's in discussion right now, conversation between industry and Congress, as it should be. And we'll stay tuned for the rest of the year.

COMMISSIONER WESSEL: Great. Thank you.

VICE CHAIRMAN CLEVELAND: Thank you. And Senator Talent?

COMMISSIONER TALENT: Yeah, just one question, Mr. Hanke. You -- I innately or just automatically sympathized with the desire of the Congress to get all the agencies together on how to define this new kind of technology.

You were, I think, critical of that, thinking that CFIUS should be able to go its own way and do its own thing for its own purposes, and I get that. But I do wonder if you don't -- if there's some other way to do it that is not going to have different standards set by different regulatory bodies for different purposes over what really is, you know, critical and important technology to the United States.

That just strikes me as inherently inefficient and there ought to be a way of efficiently coming up with a joint definition. Or what do you think, in response to that?

MR. HANKE: I agree. In a perfect world, there would be a much greater efficiency across the board in the way that we do export controls and investment screening, much greater synergy. Things would move much more quickly.

I think the challenge is that, with investment screening by CFIUS and export controls by the Commerce Department and other agencies including the State Department, we're looking at different questions.

We're looking at different types of risks. And Kevin's the expert. He can give you the three-week version on the risks involved with export controls next week.
But with CFIUS, we're talking about certain insights. When we're talking about these types of minority position investments, we're talking about insights. We're talking about access to personnel, access to information.

It's not really a pure technology transfer question. It's a different set of considerations. And so I think you've got to keep in mind that, with CFIUS, you've got nine voting members that are a part of that.

They each look at these transactions through their own lens, with their own sort of expertise. With Commerce, I mean, they're certainly the only game in town on dual use technologies, outbound at the present time.

And I think you've got to look at who brings what to the table, who should be involved in the conversation on investments. I believe it's a bigger tent than just one agency.

COMMISSIONER TALENT: Mr. Wolf, do you agree? I mean, you made the point, albeit in a different context, that it's important to have a definition for everybody to understand what it is over time, right? And that's how you get a sort of coinciding of activities. Would you agree?

MR. WOLF: Well, on the definition of national security to know what technologies to control, that's the most fundamental thing that needs to happen.

I mean, sure, there were the resource issues about why the effort was so slow the last couple of years. But I think the biggest problem was there was no vision that somebody was working to -- what outside of proliferation items do we want to control.

With respect to the specific point of your question, I testified during FIRRMA and I was a big advocate of the bill, and David and I and others worked together. But my principal comment was, if there's a technology that should trigger a mandatory filing requirement with respect to an inbound investment, a non-controlling investment, then that same technology should be regulated in a non-investment situation so you wouldn't have a situation where a company could simply sell or transfer or give away the exact same technology that triggered a mandatory filing requirement.

COMMISSIONER TALENT: Mm-hmm.

MR. WOLF: And so for that degree of efficiency was why I advocated, and a lot of others, the linking of the emerging technology process on the export side with the scope of, again, non-controlling investments.

Controlling investments, those are all under the jurisdiction of CFIUS still, even though a voluntary process. But that's a different issue.

So it's really more in the implementation, absent a definition, with the absence of sufficient resources to address the very good principle that was laid out rather than, I think, a conceptual infirmity between ECRA and FIRRMA -- in my view.

COMMISSIONER TALENT: Okay. Thank you.

MR. HANKE: Can I add one thing to that, Commissioner Talent? I think one additional point to keep in mind is that with these emerging technologies, they're just that. These are emerging technologies. They're in the cradle. These are developmental, cutting-edge.

They're hard to define. They're moving fast. It's difficult to put export controls on them. And so they're not necessarily being exported the way you'd think about technologies once they're mature. And so looking at the kinds of companies that are working on these technologies, it's difficult to define the jurisdiction based on technologies that are hard themselves to sort of categorize and classify.

COMMISSIONER TALENT: And I get the sense from the Undersecretary, and I think you mentioned this too, that their desire to work multilaterally is really slowing their part of the process down which is slowing CFIUS down, right.

MR. HANKE: Yes.

COMMISSIONER TALENT: I mean, and that makes sense too because it's always harder. That's the downside in multilateralism. It just takes a lot longer to do anything.

MR. HANKE: Multilaterally defining the jurisdiction of CFIUS is very problematic and I think --

COMMISSIONER TALENT: Yeah.

MR. HANKE: -- Giovanna's testimony about -- what was the word, disaggregating?

COMMISSIONER TALENT: Yeah.

MR. HANKE: Delinking the jurisdiction of CFIUS from the export control definition in this limited context of emerging technologies, I think, is fully appropriate.

COMMISSIONER TALENT: And that was the point you make, yes. Okay, thank you.

VICE CHAIRMAN CLEVELAND: Commissioner Scissors?

COMMISSIONER SCISSORS: Yes, Kevin, your list of what ally export controls laws don't cover was really depressing. Military/civil fusion, supply chain security, IP theft, human rights abuses, more -- what's most important for these is for elected officials to decide, hence your point about defining national security. But in line with your point too on ally adoption, I want to push you toward a recommendation.

MR. WOLF: Yeah.

COMMISSIONER SCISSORS: Just thinking about feasibility, you are a non-elected official deciding what's most important among this list of things. You're just thinking about where will the allies move most quickly, you know.

And you can define that feasibility the way you want, but I'm setting aside the true U.S. priority. You're an expert working with our friends and allies on export controls. Where would they move most quickly in that list of things they don't cover now?

MR. WOLF: Terrific question. So, even quicker, before the list is for the already controlled items and licensing policies, right now, each country can make up its own decision about whether to approve or deny an item based upon its own definition of national security.

So without any new treaties or law or legislation or change in rules outside the U.S., there can be an alignment among allies of deciding what to simply stop shipping for under broadly defined versions of national security.

So that's the quickest and the easiest. And I suspect it's happening, but it should be the aggressive. I think the next is really the civ mil fusion concept because, you know, if it has some relationship, some articulatable relationship to a military application, then you can generally convince the allies to go along with that.

But you have to have some articulation of it. It can't just be controlled because it's sensitive or control it because it's emerging or control it because it's advanced. There has to be some connection.

And so in terms -- to answer your question, there's -- I think that's the next one in terms of the list of the -- the others is going to take -- that's my sort of sea change in thinking about the role and the purpose and the use of export controls.

Because when it was created, it was created for the current system as non-proliferation tool. Chemical and biological weapons, missiles, nuclear items and conventional military items and the things that are necessary for them.

When you get outside of that, then absent a few tiny cyber surveillance systems involving human rights objectives, there simply isn't the authority in the laws of our allies now to go along with the U.S. government even assuming their political officials agreed.

So you either push the balance of what a connection is to a military application and convince them through advocacy and evidence of the civ-mil fusion issues, which I suspect has already been tried.

And at the same time, you work to get them to rethink what the role and purpose of export control should be.

COMMISSIONER SCISSORS: Thanks. I have -- I think I know Dave's answer to this question. I always want to make this point, that I saw a draft of FIRRMA at eight pages. And I hold him responsible for what happened. It started off as eight pages.

But I don't -- so I think I know what he would say, and he's given some of his answer now, but Giovanna, I'm not exactly sure I know what you would say.

There's ways to tweak the current system, fine. But how would you locate -- and I realize you have two minutes, but how would you locate definitions of critical technology? In other words, who -- you know, we have this objection to Commerce having these two kinds of technologies it's supposed to determine and then CFIUS, you know, has to wait for Commerce. But where would you -- you know, I would locate this kind of critical technology at DoD. I would, you know, in a world that you controlled, what would be the ideal way to determine what constitutes a technology that needs to be restricted in some fashion?

MS. CINELLI: It's an incredibly insightful question, Commissioner. Thank you for asking it.

So I think one of the first places I'd start is the National Strategy for Critical and Emerging technologies. In that strategy that was published in October of 2020, there was a plan laid out, albeit it was not funded and it was not articulated with any great degree of detail. But it did exactly what you just outlined with -- it's identified for national security purposed relevant to those agencies that handle defense, military and intelligence objectives -- what would be important to them.

And to a certain extent, for those of us who've been around for a while, you probably remember the old military critical technologies list and the developing technologies list that used to be maintained by Defense Technology Security Administration.

And then they, unfortunately, ran out of money in order to do that. But those lists that were tied directly to missions that were relevant to those particular objectives, hence military and intelligence, were where we would start from the perspective of what emerging and even foundational technologies would be better.

COMMISSIONER SCISSORS: And that would be agencies within the Department of Defense, then, taking the lead?

MS. CINELLI: Department of Defense, the military services, the intelligence services and I think also the State Department because they house the Directorate of Defense Trade Controls that licenses billions of dollars of defense articles and defense services every year. And they bring an overlay of foreign policy but they see the licenses, what people are requesting licenses for in that arena.

COMMISSIONER SCISSORS: Thank you.

VICE CHAIRMAN CLEVELAND: I think we all stipulate that all of Derek's questions are insightful, so we'll just -- we'll go with that. Where am I? Sorry, Commissioner Glas? Oh, wait, no, but you -- I'm sorry.

COMMISSIONER KAMPHAUSEN: Panelists, thank you very much for coming today. And I have two questions for the record. I'm going to tee them up and then invite any preliminary comment you have and then ask you to give any thoughts in response. The first is, Mr. Wolf and Ms. Cinelli, both your testimony, you talk about the need for, in varying ways, a better definition of national security. So what do you think it should be? You've identified the problem. And maybe the answer is these are the things it should include, right. But it strikes me that that's a huge benefit that we can provide to the Congress is, more than articulating the need, we actually give them some language.

The second is a little bit more provocative, but it's -- if you listen to our second panel, Commissioner Talent proposed creating a new Assistant Secretary, a structural problem to a policy challenge.

My question -- I am going to do the same. In some ways, each of you, in different approaches, have talked about the linkage of investment controls and export controls and the structural inadequacies we have in our own system.

And so the question really is, and it's more, you know, five bullet points in response to the QFR will be just fine. Japan integrates the functions, right. Japan's Ministry of Economy, Trade and Industry has bureaus for investment control and a bureau for export control.

And I've worked a fair amount with him in our IP Commission efforts. Are there merits to that in our own system? Are we -- have we built up so many antibodies to change that the process itself would be counterproductive to our national interests?

Or have we relegated roles to certain agencies? And we heard it when the Secretary Pelter talked earlier, such that there is almost an immunity to speed of action.

So I'm not suggesting we're going to -- this is, you know, a recommendation, but it merits our consideration if the structure of our system is impeding the goals that we're trying to achieve.

So any immediate thoughts on any of those? And as I said, I'll follow up with --

MR. WOLF: Yeah. And I'll send you longer answers, but on the latter one, I think there's a virtue in the current export control interagency process because there are different skills and expertise and equities at Defense, State, Energy and Commerce that they bring to a whole government solution based upon a national security direction or instruction from National Security Commission of the White House.

And so I think, if were just one agency, then -- and it's not the case that Commerce has the unilateral discretion to make any of these changes. It can't make a change of a comment -- a regulation -- without getting three other agencies to agree.

Same thing with licensing process. It's intentional an interagency concept. I have been an advocate historically for a single agency to regulate all export control issues. But that's a different topic we can into later.

On your first one, there isn't one person, I think, who has the answer to that question about what national security should mean outside the non-proliferation objectives.

I gave seven topics in my opening -- supply chain security, et cetera -- that I think warrant discussion about the role and use of export controls to address those objectives.

But it requires that same interagency collective opinion in each of the different equities of the agencies and their backgrounds to come to a whole of a government, plus evidence and information and intel that I don't have access to outside the government.

So it's a hard thing to answer in the abstract without the benefit of an interagency process with me or the access to intel or what long-term expectations are in terms of where the contrary threats are.

And then the last point is you have to distinguish between short-term economic issues and long-term economic objectives. Always, export controls will have a short-term economic impact. You're cutting off the flow of sales. You lose the money. The money goes to your foreign competitor.

But there might be longer term benefits to -- a control that need technical and economic expertise to answer. So it's hard for one person to answer your question.

COMMISSIONER KAMPHAUSEN: Maybe I'll refine the question then, to ask you to reflect on what Secretary Gates and draw from that the principles that you think ought to be applied in a future setting.

MR. WOLF: Happy to.

COMMISSIONER KAMPHAUSEN: All right, you found it compelling --

MR. WOLF: It was my intention.

COMMISSIONER KAMPHAUSEN: -- structures.

MR. WOLF: I worked for him so he told me what to do. So, yes, I --

COMMISSIONER KAMPHAUSEN: My first point, I'm a big fan of the interagency. I worry that we reify it because it's such a unique structure. It's pretty unique to the United States. And I worry that we now have made it the ideal when maybe it's not necessary. And that might be a little bit heretical, but you see where I'm going. I'm sorry, Ms. Cinelli?

MS. CINELLI: Thank you for the question, Commissioner. So let me answer your national security question first. There are some concepts that are really not subject to a definition but they are subject to an iteration of what it means in certain contexts.

I had a commanding officer who once told me that national security is whatever the mission requires. And years ago, the front page of the Military Critical Technologies List noted that there were items on that list that were quite common and readily available but still served a national security mission.

And because of that, it was very difficult to box in that a national security objective or a definition relates only to those things that are the most sensitive. It really has become more of an application-specific and end user-specific situation. You can have a safety pin that can be used to gauge an eye out, but that doesn't mean you'd want to control the safety pin. At the same time, in the wrong hands, in the wrong application, it can be an effective weapon. So there are circumstances where your actual end use and end user will be the definition of your national security process.

With respect to your second question, I think you make an excellent point, Commissioner, that the interagency process has benefits. Stakeholders bring different equities, not only their own agency missions. But they also bring and understanding of what it is that has affected the way they meet their missions. And that is invaluable when the discussions are robust. Ultimately, however, one party has to make a decision. And that party is going to overlay how it processes that information by whatever its mission is.

And we see it consistently in CFIUS, and I would like to make an observation. I mean, FIRRMA was an excellent piece of legislation. And I did find it interesting, though, that as a national security statute embedded in the Defense Production Act, it only had two whereas clauses out of 11 that related to national security.

Everything else was about the importance of investment, the importance of continuing and leaving the door open. And so the balance in the equities, both the committees that have jurisdiction, the agency that is leading the process brings that overlay to it.

And there's nothing wrong with the agency doing that. That is their mission. But what it can do in some circumstances, if there's not a counterbalance, it can diminish the equities that come from other agencies. So the interagency process has to be managed, perhaps, a little bit more efficiently as not a flat organization but one that has perhaps one or two tiers, the same way you'd organize a company.

COMMISSIONER KAMPHAUSEN: Before you answer, Dave, I want to add my thanks to that of Commissioner Wessel for your really important role and for the legislation and for the improvement of our CFIUS process when you were with Senator Cornyn.

MR. HANKE: Thanks Commissioner Kamphausen, appreciate it. On Giovanna's last point, on the whereas clause is I'll do what any good former senate staffer would do and that's blame the House side for that. That was not our fault.

But on the question about defining national security, I think Kevin's point that he made at the outset is a really good one. It's imperative to know what you're trying to do before you start doing it.

However, that's an incredibly difficult task, defining national security. And I'll give you Exhibit A. Maybe five, six years ago, the national security relevance of sensitive personal data was far less, to think that the geolocation data coming out of the app on your iPhone or maybe your personal genetic data, you know, coming from some, you know, 23andMe family genetic test might be relevant, people would be surprised by that, but that is the case.

And so national security evolves. But I think you can put into a definition what is included in national security but it cannot be exclusive because it's dynamic, it's changing. And we've got to let that happen.

Lastly and quickly, on the point about merging interagency, the processes of investment screening and export controls, I would urge caution on that. I think we've got a very good investment screening mechanism and a very mature export control system.

I think merging them together would be a bit of a mess. We've seen that movie with other agencies and, you know, it might be a solution in search of a problem. However, merging the military side and the dual use side would seem to have a lot of utility.

However, I wouldn't wish that challenge on my worst nightmare. So -- on my worst enemy, rather. That's a daunting one.

COMMISSIONER TALENT: I volunteer.

COMMISSIONER KAMPHAUSEN: Kevin, you volunteered to be his worst nightmare?

COMMISSIONER TALENT: Well, it was part of our mission when I was at the Commerce Department to merge the dual use in the military. That's -- I was referring to volunteering for combining the two agencies.

VICE CHAIRMAN CLEVELAND: So now we'll turn to Commissioner Glas.

COMMISSIONER GLAS: Thank you so much. I have a basic question here, but on the conversation about national security and the definition associated, does that require -- could the administration define what that is without congressional legislation? Or does that require a change in legislation or statute?

And then the other thing is -- first off, this panel's been incredible. The knowledge that you have and the practical experience has been really immeasurable.

But one of the questions I have is, if I'm the administration, what things could I be doing unilaterally right now based on the guidance and legislation to make the process more efficient? And what are things that Congress needs to be doing?

And I think we've heard a variety of different things today, but if our recommendations for this year's report are being formulated over the next month or so, so hearing in real time from you is really important as we're considering what the road map is that we're recommending. And I'm also happy to submit this question for the record.

MR. WOLF: I'll do the first and you do the second. So no new statute is needed to define national security. In fact, the ECRA 4817 in the U.S. Code just says the administration

should lead to an ongoing process to identify emerging and foundational technologies essential to the national security of the United States and that it limits, to the extent it's a unilateral control, to take into account foreign availability.

And so Congress created that as a separate section from the traditional national security definition which is proliferation-focused. So the law exists. The congressional mandate exists.

And going to David's point, which I agree, because national security evolves, the Congress was wise not to put in a static legislative definition. And -- but it is up to the administration to decide, which is my main point.

Until you decide what it is, even though it will evolve, it makes it very hard to decide what should or shouldn't be controlled and to convince the allies to change their thinking with respect to tech transfer of commercial technologies to China.

You guys address the second two?

MS. CINELLI: Yeah. We always get Kevin's leftovers. So let me actually comment on the second question first, which is what actions require congressional input and what actions can be done administratively.

Statutes are written fairly flexibly. That is why there's always a provision in most statutes that says, and this agency shall develop regulations because the granularity of how those statutes are going to be implemented is left to the discretion of the agencies.

What Congress does is put a remit forward about what the policy should be. And in this case, leaving national security open is actually pretty effective because, depending upon which agency is going to be implementing what aspects of the legislation, it is important to give them flexibility to bring those equities to the table.

Now, having said that, though, if things are a little bit too open-ended sometimes and too diffuse without enough direction, to Kevin's earlier point about Secretary Gates's direction about what needs to be implemented, you can get lost in the noise of even trying to figure out what you're trying to do.

And so some additional guidance from Congress about elements that it considers to be important to national security, for example, if supply chain is going to be important, then how is it going to be important and under what circumstances would be helpful.

But currently, the way the laws are structured, I agree with Kevin that there's flexibility for the administration to move forward and implement a definition. With respect to the actions that, for example, the agencies can take now, let me point to the Commerce Department. ECRA was very flexible with Commerce. While there was and is a mandate for what is controlled on the export administration regulations Commerce Control List to be based on multilateral controls, that is not always the case.

You can exercise unilateral controls in a variety of circumstances, and that is left to the discretion of the agency. There is a conundrum going on right now with what to do with emerging technologies because they're undefined or unknown yet or their application is unspecific.

Perhaps looking at the unilateral authorities in those areas, currently as drafted, those unilateral authorities, if you're putting something in, let's say, an export control Commodity Number 0Y521, I think it is. Those are limited controls. You manage it. You control it until you can figure out what to do with it and put it in another ECCN or move it elsewhere. You can exercise those uses right now of limited controls until you manage what's happening with some of the emerging technologies.

That does, of course, mean you have to know what the emerging technology is that you're looking for. And I wanted to back to Commissioner Fiedler's question to Undersecretary Pelter from the joint venture side. There actually is, right within the Commerce Department an agency called the Bureau of Economic Analysis. And they put out these reports, BEA reports they're called. There's forms you have to fill out.

One of them is a requirement for organizations to identify outward bound investments. Another one is to identify inward bound foreign direct investments. Right now, that information can be collected for statistical purposes, but the way the statute is drafted, it can't be used for any other purposes. Now Commerce may bring some of the knowledge based on what those reports reflect in the CFIUS process but currently it can't be used in any other circumstance. But it would tell us more about what's happening overseas and what's happening the U.S. that it can form and inform the authorities that the Commerce Department, in particular, has to act unilaterally. So perhaps a legislative change to that statute related to BEA may be something else to consider.

MR. HANKE: On the efficiency side, I think, with CFIUS, my advice would be to let it breathe for now. A lot has been done in tinkering with the process and in trying to make it more agile and more efficient for the transaction parties. And foreign investment is obviously very beneficial. It's a large part of the economy of the United States. We don't want to have any undue chilling effect on that.

So I think a little bit of stability there would go a long way. It's been only three years since FIRRMA was enacted and really only a year and a half since the final regulations were put in place, so that'd be my advice on that. On defining national security, staying within the CFIUS context, the underlying CFIUS statute, which is the Defense Production Act, which resides at Title 50 U.S. Code Section 4565 actually takes a crack at defining national security in a very limited way.

It just says that national security shall be interpreted to include Homeland Security -- very exciting. But it doesn't go any further than that. And I think there's probably a good reason for that. However, the same statute does include what you might call permissive factors which gives a little bit of a thumb on the scale from Congress for CFIUS to consider certain things when it reviews a transaction to determine whether or not it's problematic from a national security standpoint. So additional factors, I think, would be fully appropriate, but attempting to define it outright would be probably not a good idea.

COMMISSIONER GLAS: Thank you.

VICE CHAIRMAN CLEVELAND: Thank you all. Commissioner Fiedler?

COMMISSIONER FIEDLER: Thank you. So today we've been talking about export controls and, to some extent, CFIUS. So I will oversimplify a little bit. We have been talking about the export of things or the investment in the United States regarding companies that we don't want foreign entities to own. The concept that things are dangerous and incoming money is dangerous, I would like your opinions on whether you think that outgoing investment is potentially dangerous.

VICE CHAIRMAN CLEVELAND: Do you want to start?

MR. HANKE: Sure. I believe the Commission has had hearings on the idea of regulating outbound flows of investment from the United States into Chinese companies.
And while there are greater experts on that than myself, I do think that we need to keep in mind, as we look at the kind of companies that are being invested in by Americans, what is the practical effect on our national security.

Do we want to, in fact, subsidize state-owned enterprises that are going to be equipping the Chinese military for the next few decades in light of the challenges that we face? So that's kind of an overarching question but I believe it's fertile ground for action by the federal government. The processes that are in place now are evolving and they're relatively, I think, in their infancy. And no one should argue that they're perfect, but these are appropriate questions to as.

MS. CINELLEI: And I thank you for the question -- oh.

COMMISSIONER FIEDLER: Giovanna did -- Giovanna?

MS. CINELLI: Yes, thank you for the question, Commissioner Fiedler. I did want to comment. I agree with Dave's observations in this circumstance.

I think dangerous is perhaps a bit of a charged word. I think impactful -- foreign direct investment outside of the United States is impactful by the nature in which parties in the United States make decisions on where and how to invest.

So not only are there going to be impacts from an economic perspective; for example, the parties making the investment in the U.S. will -- from the U.S., making investment overseas, they'll gain economically from it.

But at the same time, they will provide the seed capital that's needed for the development that may not be available in the jurisdiction that they're currently in. And that is going to be double the impact that the U.S. investment overseas will have.

I think this is why it's essential, a few years ago the Commission made a recommendation in one of its annual reports -- and you'll have to forgive me, I can follow up with the year -- in which there was a question raised about whether there should be some kind of registry with, for example, the SEC about joint ventures that are registered overseas.

Not a lot of detail, but which joint venture, for what and in what country. I don't believe anyone ever looked at the issue after that recommendation with any degree of depth, but it may be interesting to resurrect that and examine whether that additional visibility overseas will answer Commissioner Fiedler's question about exactly what impact do we have from those investments that are made overseas.

COMMISSIONER FIEDLER: You know, it strikes me as we have institutionalized export controls and inbound investment oversight and consideration.

But we are using an executive order when it comes to Chinese military-related companies at the moment, which I guess, David, you're talking about as an initial move.

But what -- how would one institutionalize a process where U.S. companies, for instance, or foreign entities could be identified and U.S. companies could get clear guidance?

I mean, I'll give you an example. North Industries Group, Red Arrow company that makes missiles, rockets, caliber shells, sub-munitions owned by China North which is on the Executive Order List but North Industries, Red Arrow, is not on that list and it's continued to be owned by U.S. investors.

There seems to be this whole sort of missing system of identification that sort of threatens national security, in my view. I don't think we want rockets or missiles to be supported by U.S. investment.

MR. HANKE: If I may, I think a limited process that's focused very laser-like on a select of foreign adversary countries would be appropriate. The recent Information and Communications Technology and Services Supply Chain Screening Rule -- that's a mouthful -- ICTS Screening Rule from January by the Commerce Department, in fact, zeroes in on five specific foreign adversary country. So there's a model for doing this.

But I think some kind of interagency vetting would be appropriate in a very limited frame. And I think there could be a model there, something like the team telecom process which was also the subject of an executive order, I think, about a year, year and a half ago that reformed the process.

It reviews a much smaller number of cases and it moves about as slow as CFIUS. We would need something more agile and able to move quickly. But I think some kind of combination of those two mechanisms with a limited scope not on all countries across the world. That would be, I think, a heavy hand and unnecessary.

But I think that would be a good way to go. Do you need more than executive order? Do you need a statute? Perhaps you do. Maybe you could get the legal authority from an executive order. But I think, for Congress to weigh into this would be a perhaps beyond the realm of possibility in the next year or two. So I think an executive order may be as good as it gets.

COMMISSIONER FIEDLER: Do you see any way to reconcile the fact that any entity list companies that -- where we require licenses to trade with them could still be invested in by U.S. investors without unfettered --

MS. CINELLI: Well, I think currently there's probably two question, Commissioner, in relation to that.

There may be one set of standards for public companies and another set of standards for private companies. Public companies are more heavily regulated and they have notice obligations and filing obligations with the Securities and Exchange Commission.
And there may be some reporting obligations with respect to legal risks that they would have to include in their public filings if they were to invest in parties that were either on the Entities List or on the Specially Designated Nationals List.

Private companies don't currently have a similar formal construct where this type of reporting is required. They are responsible to their investors but that is a different situation.
So to Dave's point, it may be possible to tweak some of the processes that exist for public companies with a light touch until there's a better understanding of the impact of additional reporting but perhaps effecting the private entities.

But having said that, currently at least under the export control laws, both State and Commerce, there's not a prohibition on an investment in a foreign party except in limited circumstances and maybe some tweaking there would be helpful.

MR. HANKE: Real quick, it depends upon why the entity is on the Entity List. There are lots of different reasons. A company that's otherwise benign but was making -- shipping items to a sanctioned country or otherwise engaging in a violation but wasn't necessarily part of the Chinese Military Industrial Complex List, so the scope of listing under the Entity List is broader than the Chinese Military Industrial Complex List.

If that Entity List is engaged in contributing or supporting the Chinese Military Industry, then the standards under the executive order apply. But you can't just do a per se Entity List answer given that there are lots of different reasons why companies are on the list.

COMMISSIONER FIEDLER: Thank you very much.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Borochoff?

COMMISSIONER BOROCHOFF: Thank you. In a general sense, I just want to say that several people have touched on it, so I'm not going to ask the question, but maybe I'll send one in later. In conversations with a variety of people over on the House side, I know they're all talking about dropping bills. Ways and Means is talking about it. Foreign Affairs is talking about it.

Science Space Technology is talking about it because they're unhappy that BIS moves more slowly than they want.

So I'll be interested to hear how you all would divide things up and where you would put it. Or would you just leave it at Commerce and hope that today we get the point across?

In the meantime, I want to -- Ms. Cinelli, you mentioned something early on that really got me to thinking about the sale and transfer of technology, particularly emerging technology but anything relevant to national security which we all now know has no definition.

I'm very familiar with bankruptcies in the 80s when first all those savings and loans and then all the banks failed. I was young enough that I had no debt, so I was fortunate enough to build -- buy a lot of assets from the Resolution Trust Corporation.

And in that process, I learned a lot about Chapter 11, Chapter 13 and Chapter 7. And I think that your recommendation has tremendous merit because in particularly 11 and 7 there's a real push to just unload assets as quickly as possible in order to get a creditor satisfied.

And I can see a way, right off the bat, that a company could game that system just to transfer the technology. So that's a wonderful recommendation and I think it bears great merit.

I have a question though, since you brought that up and I don't know the answer. Is there a control over a private company that's not in bankruptcy transferring something that maybe has not been yet decided to be a national security issue?

MS. CINELLI: So I think that would depend on to whom they wanted to transfer it to. Within the United States, there really are very few limits --

COMMISSIONER BOROCHOFF: Right.

MS. CINELLI: -- between two private parties. If they wanted to transfer it to a foreign party, if the technology is not subject to any current jurisdiction of any agency, then, candidly, Commissioner -- and it's an excellent question -- it's a gap.

There is no visibility. There's no permission, there's no requirement. There is a slight overlay that if that technology is subject to intellectual property, if it's part of a patent, if it's trade secrets -- in the trade secret context you may have some kind of repercussions if you did that, but otherwise, no.

COMMISSIONER BOROCHOFF: So my follow-up to that, then, is you talked a little bit about catch and release. And you used a little bit different technology and called it hold and release or hold and -- I don't remember the other word -- same concept.

Let's say that somebody invents something that has great medical use, would also be applicable to save money in manufacturing and engineering but lastly has direct weaponry technology. How long is a typical catch and release before that product gets to hit market? I know everybody says this all takes time, but what would you recommend to somebody who came to you and said, I want you to consult for me. I've got and invention. When do I get to bring it to market?

MS. CINELLI: Yeah, again, an excellent question. And when you're asking for timelines, it's always driven by the circumstances. So for the product that you were talking about, for example, it isn't so much a question of restricting it but as it is of knowing who's going to use it for what application.

COMMISSIONER BOROCHOFF: I see.

MS. CINELLI: So you may want to put it on a list, assuming you're keeping a list, and say this technology has three different applications. When it is this application, here is the process for sharing. When it's this application, here is the process. And when it's this application, you have to come in for a license.

The challenge there -- and it goes back to my impact on business --

COMMISSIONER BOROCHOFF: I know.

MS. CINELLI: -- is I have the direction, but that puts the burden almost completely on the business to do all the diligence, to know their end user and know the application of it.

COMMISSIONER BOROCHOFF: And they have to restrict their end user, right?

MS. CINELLI: Exactly. Exactly.

COMMISSIONER BOROCHOFF: So, you know, if you sell something to a cosmetic company, likelihood is they're not going to sell it to China to be used for a weapon. But if China is aware of the possible use, we don't have a way to restrict that today, do we?

MS. CINELLI: Right, and that is the big challenge. That's where the equities come in. So what I think Congress needs to provide some guidance on is where do you put that shifting line?

You know, to say that it's too difficult to process and therefore nothing can be controlled, I would suggest to both the Commission and Congress, that is not helpful to the United States or to any of its objectives. On the other hand, you don't want to throttle and strangle technologies and sharing, but at the same time, if there are time limits for the periods of control that happen, then maybe that is a potential compromise now.

And that is something that I think merits further study. But simply keeping the process as is and saying it's difficult to get multilateral agreement, I'm not sure is helping anyone, certainly not industry, not the administration and certainly not the objectives of the statute.

COMMISSIONER BOROCHOFF: Thanks for bringing that to our attention.

MR. WOLF: Just a quick follow-up. There are, by the way, what are called catch-all controls since the early 1990s that the allies agreed to that if there is knowledge that an otherwise uncontrolled technology is used for the development or production of chemical or biological weapons, nuclear missile and now military intelligence applications, even for unlisted technologies, once that knowledge exists, a regulatory requirement kicks in. And that is a multilateral control that has been in place for several decades now.

COMMISSIONER BOROCHOFF: And, I'm sorry, I'm overtime. Does that, if it's U.S. origin technology it attaches to the technology forever --

MR. WOLF: All the way through.

COMMISSIONER BOROCHOFF: All the way through?

MR. WOLF: If it's the cosmetic company from -- if it were U.S. origin from the United States then jurisdiction would apply.

COMMISSIONER BOROCHOFF: Great.

MS. CINELLI: If I could just add, it does require knowledge though.

COMMISSIONER BOROCHOFF: It requires knowledge.

MS. CINELLI: And that means a level of diligence and what constitutes knowledge. I mean, there's civil standards and there's criminal. But I think there are some opportunities. It's just not -- it's a little bit messy.

COMMISSIONER BOROCHOFF: Very frightening to be asked what did you know and when did you know it. I understand.

VICE CHAIRMAN CLEVELAND: Thank you. Commissioner Bartholomew?

COMMISSIONER BARTHOLOMEW: Thanks. And thank you to our witnesses. This is interesting and your ability to take this very technical issue and make it more comprehensible for those of us who are not experts in it is very welcome.

I guess it's a variation on what Commissioner Kamphausen was asking about, and I'll stipulate that I believe that we need strong controls. And, you know, I appreciate that there's a process that the government is going through.

But I just wonder, Mr. Hanke, you used the word agility. And I just wonder, given the pace of change in technology, how we can help our bureaucracy be more efficient and more agile in responding to these challenges.

You know, every time I hear interagency, I think that's great, but that slows things down. Every time I hear multilateral, I think that's great, but that slows things down. Even more, the regulatory process, you know, in terms of issuing regulations, I mean this can take months if not years on some of these technologies and things move on. So are there things that we can do that would increase the agility of our bureaucracy to be able to deal with these things? That's any of you.

MR. HANKE: Kevin might be well-situated to talk about the nooks and crannies of actually trying to do that when he was at BIS years ago. But, you know, not all emerging technologies are appropriate for control. There's a certain point at which they're mature enough and there's a variety of factors that go into the decision when you actually want to impose a control. And in so doing, you'd only want to do it on a temporary basis. You'd want to then pursue multilateral controls as soon as you could so that the company would not be disadvantaged for the long run.

But, Kevin, you invented the 0Y521 concept, I believe, so maybe you want to put more meat on the bone there.

MR. WOLF: So the biggest -- I think as slow as the interagency is, it's worse than the alternative. It's all about the least bad options.

If you just have one person or one group with one degree of expertise, you're not going to get a whole of government response. And so it really is a function then, not of the -- it's not a problem. In fact, there's a virtue in interagency clearance because people have different backgrounds and expertise. It's given that we're dealing with a new type of national security issue.

The system wasn't designed for that. And there are really, really talented people in the U.S. government, in the export control agencies. And if you get into an electronic warfare system application or a military system or Stealth technology application, world's leading experts can track down all the way through the root cause and the commercial technologies that are critical to it.

And, but when you start getting into areas that don't come from the weapons world or the proliferation world and the AI or quantum or robotics of exclusively commercial semiconductors, the system wasn't really designed.

So the best thing Congress can do is to get people who are experts in that area, you know, not necessarily from a traditional proliferation or military background, into the U.S. government. Encourage them to want to become a licensing officer or policy officer at Commerce, State, Defense. And it's really recruiting and a new way of thinking is the critical exercise.

I don't think the answer is to eliminate the multi-agency, inter-agency process. And to come to the defense of BIS, by the way, with respect to some of the other comments, the Bureau is there as the coordinator of a broader interagency system to pull together for a whole of government perspective on what the rules are and then to be industry-facing.

Its purpose is to be the industry that faces industry with respect to the regulatory and the licensing process because all of the issues about interpretation, about what's caught or not, you need someone who's an expert in administering the system.

And that doesn't mean you don't take into account the expertise from the Defense Department or the State Department or the Energy Department or other departments.
So I really -- I'm sorry it's a -- everybody always asks for more money, but I'm no longer in government so I can't. It really is a dramatically expanded amount of resources for the five agencies that are responsible for this. And not just money for the sake of money, but for the sake of recruiting people that have backgrounds in these technologies that are really at heart so that the questions can be understood and the actions can be a lot more quick as a result. They're, frankly, overwhelmed.

COMMISSIONER BARTHOLOMEW: Yeah, and again, I didn't do this to say -- ask this question to critique the people who are trying to do their best in these circumstances, but Kevin, do you think it would be helpful to sort of have a list of the kinds of talent that they need to be recruiting for? Do they know?

MR. WOLF: Absolutely. A position description should be drafted. You know, Bill Nye already has a job so you can't hire him. But it has to be other people who have, you know, expertise in each of these areas. And with the funding for position descriptions outside the traditional, that would be a really good practical first step.

And with the -- and then, and by the way, I would also advocate direct hiring authority. Congress did a great job with FIRRMA, at giving CFIUS the ability to beef up its personnel with more money and the ability to hire people more quickly.

The existing system within the government for getting people into the government takes a year. It's very complex. And I would advocate going straight to being able to hire the people that are needed who have expertise and background in these areas.

COMMISSIONER BARTHOLOMEW: Great, thanks so much.

VICE CHAIRMAN CLEVELAND: Thank you all. Giovanna, I'm interested in your written testimony where you note that -- and you mentioned it also in your oral testimony -- that the Secretary of Defense has the ability under this Critical Technologies List to inform a number of federal decisions -- and including but not limited to any interagency determination conducted pursuant to federal law relating to technology protection, including export licensing, deemed exports, tech transfer and foreign direct investment.

So I have not read the underlying statute, but what I'm interested in and it may be relying on a very dated experience at CFIUS for me, if the Secretary of Defense said something on that list of 38 emerging technologies was of concern, what's the impediment to bringing that into CFIUS?

Because my experience was on a weekly basis. DoD was saying we need to be discussing X, Y or Z in CFIUS. And it was a constant process of saying explain why and what. It seems now CFIUS, through whatever, for whatever reason, has been cabined in some way where there are barriers or impediments. So I'm just curious to sort of what's happened over the years. And if the Secretary of Defense says this is critical, what impedes CFIUS from discussing, debating and taking action?

MS. CINELLI: So that's an excellent question. Thank you. I think there's two points. One, the Committee, in order to have this discussion with Defense, has to have something under its jurisdiction that's under review. So if there's a transaction that it's looking at and the technology's involved, of course Defense will bring the equities to the table. They'll discuss it.

And that's why we have mitigation agreements and that's why we sometimes have presidential orders for divestment or denial. So I think in those circumstances there is robust discussion. There is engagement. And the interagency process works.

There's also, as I understand, an escalation process so if there's some form of misalignment, in the views, there's a process for escalating where ultimately a decision is made.

And I think that, to Dave's earlier point, those types of processes work well. I think part of the concern sometimes is the agency and group within DoD that is developing the Critical Technologies List may not be the group in FIRS, the Foreign Investment Review organization. And how does that intra-agency communications process work to bring those equities over? I would suggest that, based on some of the transactions we've seen where the Committee has reached out and requested what's called a non-notified filing, that aspects of that process are working quite well.

But then there is inconsistencies where transactions, as you look at them, perhaps raise some concerns and no one inquires about it no filings are made, so --

VICE CHAIRMAN CLEVELAND: Because no government is perfect. But I'm -- you've gotten at the issue that I'm interested in, which is the non-notified.

And so, it would be accurate to say that there is the opportunity for CFIUS based on whether it's the critical -- and the intra-agency process as such that DoD, given the weight of DoD, raises issues beyond Critical Technologies List.

So I guess I'm really asking for sort of a simple -- because this is very complicated for me. If DoD came in and said that they were aware that Company Xi -- X was looking at investing in Bob's cosmetic company that has the potential to -- yeah, to create a bio-weapon of some sort -- if DoD came in and said American company has this capability.

We are seeing overtures or concerns, this is something that we view as a threat to national security, is there a legal or a regulatory or a rule, restriction or barrier that keeps CFIUS from seeking information from that company?

MS. CINELLI: So the short answer to the question is no, not per se.

VICE CHAIRMAN CLEVELAND: Right.

MS. CINELLI: And so if it is a transaction that is underway or a transaction that has occurred and that's what DoD's view is, it's likely that that transaction will end up on the Non-notified List.

VICE CHAIRMAN CLEVELAND: Right.

MS. CINELLI: But FIRRMA expanded the development of Non-notified List to Treasury as well. There's a request for Treasury to do the same thing, to keep a list of non-notified transactions.

And it may be that perhaps in the interagency process overall, if any agency came up with something that was similarly impactful, they should be able to bring that to the attention of the Committee and indicate there needs to be a non-notified outreach.

VICE CHAIRMAN CLEVELAND: Right.

MS. CINELLI: The question, and I don't have an answer to this. Perhaps Dave and --

MR. HANKE: Yeah, I --

MS. CINELLI: -- Kevin might. The question is all the outreaches come from Treasury. So when those circumstances, when Defense makes a request and says this is problematic, for example, it is not, as I understand the process, something where Defense reaches out independently in the CFIUS process.

VICE CHAIRMAN CLEVELAND: Right.

MS. CINELLI: That is something that goes through Treasury. The question I have is what if Treasury disagrees with that assessment.

VICE CHAIRMAN CLEVELAND: So I think we're now getting into sort of soft territory of speculation. My experience was you'd be hard-pressed to disagree if DoD came in and I would also say DoD came in all the time, often with things that many of us didn't agree with.

But the non-notification process is not, in and of itself, risky or a threat. It is an inquiry to determine whether there's a basis to proceed.

And so what I appreciated and what you had to say, Mr. Hanke, about creating institutions, organizations or bureaucracies that add to the problems, and some of us take the view that Homeland Security may have contributed to just such an outcome, I want to be really careful in terms of how we perceive it as a group -- and obviously, everybody has a point of view -- that we not break something that has inherent authorities to protect from the riskiest of transactions.

And so in my mind, when I look at that list of 38 -- was it 38 emerging technologies -- which are broad, I almost feel that's sufficient, that that is guidance, that we are never going to get to a better space of -- within each of those categories there will be 43 more technologies under each of those headers.

That, if I was sitting at CFIUS, at any of the agencies, I would say, okay, here's my guidance, just like your national security guidance. I'm going to use this to pull in transactions, non-notified or otherwise, because this gives me some sense of where the real concerns are based on the administration's concerns. What's wrong with that approach? What would we miss? What would get overlooked?

MR. WOLF: Sure, three quick comments. So in terms of the outreach for information from CFIUS, I agree with everything that you said.

There's also another thing that David mentioned earlier which I created in 2012, which is this 0Y521 process which I created because what if we made a mistake in not controlling something that should?

What is there was an emerging technology which we put in the rule which became the precursor to the statutory provision?

I wanted to be able to have the very quick authority to impose unilateral control to regulate it. And never once did Defense request something that we didn't agree to.

VICE CHAIRMAN CLEVELAND: Right.

MR. WOLF: Same thing, I was on CFIUS for seven years. I reviewed a thousand cases. Never once did Treasury ever refuse a Defense Department request to ask a question about a potential non-notified or other transaction.

So I think that's a theoretic -- I don't know about the last four years, but I doubt ever there was a Defense request that didn't go unanswered.

So to answer your primary question, the legal authority already exists to do what you want in gathering information or to have a very quick unilateral control. You could either do it under the regulations or the new statute that we were talking about.

The thing that you have to be careful about in that, in too broad of a control, is creating a fear and uncertainty because uncertainty is death to trade.

VICE CHAIRMAN CLEVELAND: Right.

MR. WOLF: I mean, foreign investment is critical to the United States. We want to encourage benign investment. And the tension is between the discretion that you want to be able to know it when you see it in terms of something that had broad categories of technologies to control and making it so aggressive and so uncertain and so unclear that investors simply want to avoid the U.S. because it's more trouble than it's worth.

Investment doesn't come in, a U.S. company doesn't get the income to do the R&D to out-compete its foreign investors. The income goes and the investment goes to their competitors overseas. We lose the advantage with our U.S. industrial base as a result of the loss in that investment.

So that's the biggest -- and that's why I think ultimately the FIRRMA/ECRA compromises and tradeoffs, while it's not perfect from a national security perspective and it's not perfect from a free investment and free trade perspective, at least it brought stability and certainty.

And my number one advice, whatever you do, whether it's hard or soft, tough or weak, is that it is certain and clear, going to Giovanna's point earlier about the regulations.

And if people don't know what's controlled or not, they will simply avoid the United States over time. I mean, not initially, but eventually you create structural incentives to avoid the U.S. And that ultimately hurts our national security because it hurts the economic security.

So that's -- those are the three responses to your question. I hope I answered them.

VICE CHAIRMAN CLEVELAND: It did. And I think the interesting watch word for the Commission this year is the word disentanglement. We tend to focus on decoupling, but I think that we need to think more deeply about what does it mean to disentangle and the ideas of ECRA and FIRRMA.

It came up in the hearing that -- Commissioner Wong talked about it with Commissioner Fiedler -- disentangling conventional versus nuclear. It is, I think an interesting sort of framing of how we think about the relationship with China. I think, unless anybody has additional questions -- no? Yeah? No? Okay, I think we're done for the day. I want to thank Emma and again, Alex, your last hearing, well done -- and Charles and the rest of the staff for preparing us well.

We really appreciate it and thank you all for testifying. You took a very complicated issue and -- our mistakes are our own after this. How about that? So thank you.

This is the last hearing for the year. Is there anything else I need to say, do? No? That's it. So thank you all. Take care.

(Whereupon, the above entitled matter went off the record at 3:41 p.m)

QUESTION FOR THE RECORD

RESPONSE FROM JEREMY PELTER ACTING UNDER SECRETARY FOR INDUSTRY AND SECURITY, BUREAU OF INDUSTRY AND SECURITY, U.S. DEPARTMENT OF COMMERCE

UNITED STATES DEPARTMENT OF COMMERCE
Under Secretary for Industry and Security
Washington, D.C. 20230

September 8, 2021

Response to Question for the Record (QFR)

Jeremy Pelter
Acting Under Secretary for Industry and Security
Bureau of Industry and Security, U.S. Department of Commerce

Testimony before
the U.S.-China Economic and Security Review Commission

Hearing On
"U.S.-China Relations in 2021: Emerging Risks"

QUESTION:

Your written testimony shows a very sharp increase in enforcement actions by Commerce in FY21 over FY20. Can you explain the increase? Is it due to much greater enforcement efforts, an oddly timed jump in violations, or something else?

ANSWER:

While no single issue accounts for an increase in enforcement actions by the Bureau of Industry and Security (BIS), which are tied to the timing of leads and export transactions, there are likely multiple factors that contributed to the larger number of actions and penalties in FY21. First, COVID-19 closed many courts during FY20, which delayed some cases and sentencing hearings until FY21. Additionally, BIS continued to assume export control jurisdiction over more items and thus enforcement of more export transactions. This includes exports of certain firearms and related items that moved from the jurisdiction of the Department of State to the Department of Commerce in the middle of FY20. BIS's enforcement team also has continued to expand its geographic footprint to reach more exporters and potential leads of noncompliance with BIS export controls. BIS continues to aggressively enforce export controls related to China, including the significant expansion of controls that occurred in FY20 and 21 related to military end users/end uses, military-intelligence end users and end uses, and additional parties on the Entity List. Moreover, the Office of Chief Counsel for Industry and Security continues efforts to amplify its support of BIS enforcement actions to appropriately hold violators accountable.