U.S.-China Economic and Security Review Commission Hearing:

"Key Economic Strategies for Leveling the U.S.-China Playing Field: Trade, Investment, and Technology"

Panel 2: "Measures to Limit the Flow of Key Technologies to China"

Testimony of Peter E. Harrell

May 16, 2024

Members of the Commission, it is an honor for me to testify on the topic of today's hearing, "Key Economic Strategies for Leveling the U.S.-China Playing Field: Trade, Investment, and Technology." The views I express today are my own and I am not here speaking on behalf of any organization.

The Commission plays an important, bipartisan role in identifying economic and national security challenges in the U.S.-China relationship and in making recommendations to Congress regarding U.S. policy towards America's leading strategic competitor. To cite just a few recent examples, the Commission has been instrumental in making recommendations on export controls, restrictions on both outbound American investment to China and inbound investment from China, trade policy, and on the risks posed by the use of certain Chinese technology, such as telecommunications technology, in the United States.

Of course, as Commissioners know well, more needs to be done to position the U.S. for today's era of strategic competition. The most recent U.S. National Security Strategy, released in October 2022, describes China as "the only competitor with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to advance that objective."[1] China is endeavoring to modernize its military so that it can threaten U.S. allies in Asia and push U.S. military forces out of China's near abroad. Beijing is increasingly aggressive towards Taiwan, and the U.S. must be prepared for a potential military conflict in the Taiwan Strait in the years ahead. Beijing is continuing its years-long quest to secure control of critical global supply chains and to build the industrial capacity and technological know-how to dominate the essential industries of the future.

Against that backdrop, I will spend my testimony today discussing three broad topics:

- First, the lessons from recent U.S. export controls on China and Russia.
- Second, the need for a more comprehensive strategy when it comes to limiting technology flows between the U.S. and China.
- And third, the need for a better framework for restricting high-risk technology imports from China and high-risk U.S.-China data flows.

[1] The White House, "U.S. National Security Strategy," Oct. 2022, https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

Lessons from recent export controls on China and Russia:

Over the last five years, the United States and our allies have embarked on two major campaigns of export controls. The first of these is an increasingly comprehensive campaign to control the export of semiconductors and semiconductor manufacturing equipment to China. The second of these is the sweeping campaign of sanctions and export controls that the U.S. and our allies have imposed on Russia since its invasion of Ukraine in February 2022. Both these cases offer important lessons for the U.S. as we consider the role of export controls in maintaining our strategic edge over China.

Former President Trump began the current campaign of semiconductor-related export controls in 2019 when his Administration imposed restrictions on Chinese telecommunications company Huawei in a bid to erode its growing presence in international telecommunications networks. The Trump and the Biden Administration subsequently added a number of other specific Chinese companies, such as semiconductor manufacturer SMIC, to America's targeted export control lists. Then, in October 2022 President Biden expanded this campaign by deploying an innovative set of country-wide controls on China, which the President further broadened in October of last year.

Broadly speaking, the controls that the U.S. has imposed on exports to China of advanced semiconductors and semiconductor tooling starting in October 2022 have the hallmarks of a successful export control strategy. They built on the earlier experience of export controls targeting specific Chinese firms, which were proving increasingly difficult to enforce given China's opacity and the prospect for diversion and workarounds within China. The export controls have clear objectives: slowing the development of China's semiconductor and AI technologies, both of which are quintessential dual-use technologies that China could deploy to strengthen a range of military applications. The export controls leverage chokepoints by focusing on products that China cannot readily source domestically.

I see the iterative process of the semiconductor export controls, expanding from firm-based to country-based in 2022 and then expanding again in October 2023 to cover additional types of semiconductors and equipment, as a strength, not a weakness, of the export controls regime. Export controls will almost always be an iterative process and the United States should expect to regularly update and expand export controls to address gaps and workarounds as they are identified. Starting a new export controls regime with a comparatively narrower set of controls and expanding them over time allows policymakers to identify strengths and weaknesses, address gaps, and reduce the odds of unintended consequences, which could be significant, particularly with respect to China, given China's economic scale.

The U.S. has also been broadly successful in convincing key like-minded jurisdictions that produce semiconductors and semiconductor manufacturing equipment, notably the Netherlands and Japan, as well as companies in Taiwan and South Korea, to join the U.S. in imposing broadly similar export controls, constricting China's ability to source products from non-U.S. suppliers. Admittedly, there has been significant discussion in the export controls community and in industry regarding the fact that the U.S. initially imposed controls on semiconductor manufacturing equipment before Japan and the Netherlands, and of the fact that aspects of the U.S. controls continue to go further than do allied controls: For example, U.S. allies have so far not joined in restrictions on their citizens servicing semiconductor manufacturing equipment already in China. However, the practical

diplomatic reality is that sometimes the U.S. has to impose controls first, before getting allies and partners on board: diplomatic experience shows that allies and partners may prove unwilling, for their own internal political reasons, to act until they see that the U.S. has done so. So long as the U.S. government is actively engaging with key allies to seek further alignment and has a plausible strategy to obtain such alignment, the U.S. should not be afraid to act first.

Let me now turn to Russia. In late 2021 and early 2022 the U.S. and its G7 allies sought to use the threat of sanctions and export controls to deter Russian President Vladimir Putin from attacking Ukraine. After Putin attacked in February 2022, the U.S. and our allies imposed sweeping sanctions and export controls on Russia in a bid to both deprive Russia of revenues and to degrade Russia's industrial base and capacity to wage its war of aggression. Currently, U.S. and our allies impose export controls on a wide range of products including semiconductors, manufacturing equipment, dual-use technologies, and numerous chemicals and materials, among other products.

While the threat of this campaign of sanctions and export controls failed to deter Putin and has not prevented him from waging his war on Ukraine, in my view the sanctions and export controls have been useful in eroding Russia's military industrial base. For example, a detailed analysis by the Kiev School of Economics published earlier this year found a sharp drop-off of both "battlefield goods" and "critical components" after the imposition of export controls in 2022. While there has been a significant rebound as Russia developed new suppliers, in late 2023 Russia's imports of battlefield goods remained about 10% below their pre-war levels while its imports of critical components remained about 29% below pre-war levels.[2]

Indeed, in December of last year Ukrainian President Volodymyr Zelensky stated that Ukrainian intelligence was seeing a "deceleration" in the Russian defense industry even as Russia was able to continue the war.[3] Moreover, it is hard to imagine that Putin would have turned to Iran and North Korea to provide drones, artillery shells, and other military equipment if his own defense manufacturing base was working as effectively as his military would like. To be sure, by far the most important element of defeating Putin's war of aggression is the military support the U.S. is providing to help Ukrainian soldiers on the battlefield. But a continued campaign of sanctions and export controls can help erode Russia's war machine.

When I look across these two cases, I see multiple lessons relevant to the future of U.S. export controls on China.

First, the October 2022 shift from controls focused on specific Chinese firms to controls directed at China as a country marked an important strategic pivot. The opacity of China's market, the opportunity for transfers and to divert export-controlled goods between entities within China, and China's civil-military fusion strategy all make it likely the U.S. will need to deploy country-wide export controls in future campaigns against other critical elements of China's technology sector. To be sure, entity-based export controls will always be important to call out the harmful activities of

[2] Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk, and Vladyslav Vlasiuk, "Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production," *Kiev School of Economics*, January 2024, p. 8, https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf.

[3] "Intelligence suggests slowdown in Russian military industry — Zelenskyy," *New Voice of Ukraine*, Dec. 21, 2023, https://www.yahoo.com/news/intelligence-suggests-slowdown-russian-military-214500632.html.

specific firms and as a way of restricting exports to Chinese companies operating in third countries, such as Southeast Asian countries. But I expect that the U.S. and our allies will increasingly need to impose country-wide controls to address diversion risks and to ensure that export controls are successful in advancing strategic objectives.

Second, I recommend that the U.S. and its allies minimize the time lag between signaling or announcing export controls and the actual effective date of such controls. There is significant evidence that Huawei was able to use the lead-up to the Trump Administration's well-signaled 2020 export controls against the company to stockpile western semiconductors, blunting the controls' impact in the months after came into effect.[4] Similarly, publicly available trade data suggests that last year Chinese semiconductor manufacturing firms used the months before implementation of Japanese and Dutch controls on semiconductor manufacturing equipment to speed up equipment purchases.[5] This, too, will likely undermine the effectiveness of the controls in the short term, although the benefits of stockpiling fade over time as firms run through their stockpiles. (The export controls that the U.S. and its allies imposed on Russia generally had much shorter implementation periods).

Third, the government needs to do a better job of integrating its sanctions and export controls tools. After the U.S. and G7 allies imposed export controls on Russia in 2022, Russia pivoted to China and a handful of other countries, such as Turkey, to procure replacement goods. To address the flow of dual-use goods from these countries to Russia, in December 2023 President Biden issued an Executive Order (E.O. 14114) authorizing the Treasury Department to impose sanctions against third country banks that facilitate the sale of dual-use goods to Russia. While recent trade data show that many Chinese exports to Russia are continuing, the data also suggests that the E.O. is having a useful impact: for example, earlier this year Chinese exports to Russia appear to have modestly fallen after rising for most of 2023 (albeit off of lows in 2022).[6] The U.S. government should explore mechanisms to build on this precedent to reinforce the potency of U.S. technology export controls on China. For example, an Executive Order or congressional sanctions program could authorize sanctions against companies in countries that do not participate in U.S.-backed export controls when those companies sell high-end semiconductors or semiconductor manufacturing equipment to China, as well as against institutions that facilitate such sales.

Fourth, the failure of sanctions and export controls to deter Vladimir Putin from invading Ukraine leaves me skeptical that the threat of sanctions and export controls will deter Beijing from attacking Taiwan or a U.S. ally such as the Philippines, if Xi Jinping decides that he needs to deploy his military to achieve an objective he views as essential. In those circumstances, I fear that Xi, like Putin, may view sanctions and export controls simply as a price to be paid. This is not to say that the threat of sanctions and export controls cannot change Chinese behavior; but we cannot count on them to succeed as a last-ditch deterrent to military conflict.

---

[4] See, e.g., Lauly Li and Cheng Ting-Fang, "Huawei builds up 2-year reserve of 'most important' US chips," *Nikkei Asia*, May 28, 2020, https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-builds-up-2-year-reserve-of-most-important-US-chips.

[5] "China Buys Near Record $40 Billion of Chip Gear to Beat U.S. Curbs," *Bloomberg*, Jan. 22, 2024, https://www.bloomberg.com/news/articles/2024-01-22/china-buys-near-record-40-billion-of-chip-gear-to-beat-us-curbs?sref=HblxZSKM.

[6] See, e.g., "China's Exports to Russia Slump Amid US Threat of War Sanctions," *Bloomberg,* April 16, 2024, https://www.bloomberg.com/news/articles/2024-04-16/china-s-exports-to-russia-slump-amid-us-threat-of-war-sanctions?sref=HblxZSKM.

In my view, the most important deterrent to Beijing engaging in military adventurism is Beijing's concern that it would fail to accomplish a military objective—that, like Putin, Beijing would face either a protracted military struggle or an outright military loss. This leads me to my next recommendation: that the U.S. undertake a comprehensive review of our sanctions and export controls to identify chokepoints that can further slow China's military development.

Of course, the U.S. and our allies have long prohibited the export of military technologies to China and have restricted the flow of dual-use technologies to Chinese military end users and end users. U.S. semiconductor export controls are intended to slow China's military advancement. But China's military development does not rely only on military technologies and on semiconductors. It relies on a range of both emerging high technologies—technologies such as autonomous flight systems, quantum computing, sensors, and robotics—and on more traditional military industrial base sectors, like aerospace. The U.S. should undertake a comprehensive review of potential technological chokepoints across the Chinese military industrial base, and, working with allies, deploy export controls and other tools to leverage those chokepoints to slow China's military advancement.

A fifth lesson from U.S. export controls on Russia and China is the need for effective implementation and enforcement. In the years after the 9/11 terrorist attacks, the U.S. Treasury Department and global banks undertook a years-long campaign to radically overhaul the way both the Treasury and the private sector enforced U.S. sanctions: expanding customer due diligence; developing systems to spot, report, and, when appropriate, stop, suspicious transactions; and to harden the financial system against the flows of terrorist finance. We need a similar long-term initiative with respect to export controls to strengthen corporate compliance, improve information-sharing between companies and the government, and appropriately resource export controls offices across the U.S. government.

Indeed, there is some evidence that stopping smuggling and improving compliance by western firms could be at least as important as cracking down on third country suppliers, like China. The Kiev School of Economics' January 2024 report on export controls found that of 2800 different non-Russian components that experts recovered from from Russian weapons in Ukraine, almost all of the components—95%—originated from Western firms, with only about 4% of them originating from Chinese firms.[7] Many of these components were likely manufactured by western firms in third countries, including China, where they disappeared into shadowy networks of middlemen. But the fact that components made by western firms remain so overwhelmingly common inside Russian weapons suggests that companies and government can and should work together to strengthen compliance.

Particularly given that export controls often involve physical goods, the government and private sector should develop better physical traceability mechanisms for sensitive goods. For example, recent press reports have described the smuggling tactics that Russia deploys to source replacement

[7] Olena Bilousova, Benjamin Hilgenstock, Elina Ribakova, Nataliia Shapoval, Anna Vlasyuk, and Vladyslav Vlasiuk, "Challenges of Export Controls Enforcement: How Russia Continues to Import Components for Its Military Production," *Kiev School of Economics*, January 2024, p. 5, https://kse.ua/wp-content/uploads/2024/01/Challenges-of-Export-Controls-Enforcement.pdf.

parts for its civilian aviation fleet, which still consists largely of Boeing and Airbus aircraft.[8] Physical geolocation tracking tags with built in "kill switches" could, over time, make it much harder for Russia to procure such parts, or for China to covertly source semiconductor manufacturing equipment.

Before turning to remarks on the need for a comprehensive technological control strategy, I want to speak for a moment about the costs of export controls.

Increasing the number and variety of U.S. export controls and the scope of compliance expectations will create costs for U.S. businesses. A company spending millions of dollars on export controls compliance is not spending that money on R&D, investment, or returns to shareholders. A company that loses out on a market opportunity will not build a factory here in the U.S. to serve that demand. If the U.S. acts too unilaterally in too many export controls cases, the U.S. does risk creating incentives for foreign firms to design out U.S. components, ultimately weaking both American companies' market position and the power of U.S. export controls.

Yet while we should always weigh these costs carefully, we also should not over-weight them. Reports by Bloomberg and the Atlantic Council (among others) show that the costs of a cross-strait conflict between China and Taiwan would be catastrophic for the global economy, likely inflicting trillions of dollars of economic damage.[9] Preventing such a conflict has enormous economic value, not to mention the value of preserving the international order. A Russian victory against Ukraine would necessitate hundreds of billions of dollars in additional U.S. and European defense spending to ensure that Russia could not leverage victory in Ukraine into an attack on a NATO ally. Failing to impose export controls can carry costs, too.

Moreover, calculating costs is complicated as markets are dynamic. Cost calculations are not simply a matter of calculating the value of U.S. exports of a widget and assuming that that will be cost of an export control on that item—in many cases markets may adjust, particularly with respect to China, which multinational companies are already diversifying away from. For example, according to the Semiconductor Industry Association (SIA), approximately 29% percent of global semiconductors are sold in China.[10] Certainly, the prospect of losing access to 29% of the global market would be damaging to most firms. But as SIA notes, a large share of the semiconductors sold in China are incorporated into products assembled in China but ultimately exported to the world. As electronics supply chains diversify away from China in the coming years, it is reasonable to expect that China's share of global semiconductor sales will decline.

---

[8] Chris Cook, Sylvia Pfeifer, Polina Ivanova, and Chloe Cornish, "The smuggling trail keeping Russian passenger jets in the air," *Financial Times*, May 10, 2024, https://www.ft.com/content/f8d61a5d-708f-47c4-8dbd-0e80452dea5a.

[9] *See* Jennifer Welch, Jenny Leonard, Maeva Cousin, Gerard DiPippo, and Tom Orlik, "Xi, Biden and the $10 Trillion Cost of War Over Taiwan," *Bloomberg*, Jan 8, 2024, https://www.bloomberg.com/news/features/2024-01-09/if-china-invades-taiwan-it-would-cost-world-economy-10-trillion?sref=HblxZSKM; Charlie Vest and Agatha Kratz, "Sanctioning China in a Taiwan crisis: Scenarios and risks," *Atlantic Council*, June 21, 2023, "https://www.atlanticcouncil.org/in-depth-research-reports/report/sanctioning-china-in-a-taiwan-crisis-scenarios-and-risks/.

[10] Semiconductor Industry Association, "2024 Factbook," May 14, 2024, p. 10, https://www.semiconductors.org/wp-content/uploads/2024/05/SIA-2024-Factbook.pdf.

This is why I recommend that the Commerce Department expand its capacity to rigorously analyze and model the expected costs of U.S. export controls. Last year, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), which administers U.S. financial sanctions programs, created an Office of the Chief Economist to help OFAC and the U.S. government better evaluate both the impacts and potential costs of U.S. sanctions. The Commission should recommend that Congress direct the Commerce Department to establish a similar unit at the Bureau of Industry and Security to conduct economic analysis with respect to U.S. export controls.

Towards a comprehensive strategy for export controls:

In the interest of time, I plan to offer more concise remarks on the two remaining topics I will address today: the need to develop a comprehensive strategy for U.S. export controls on China and the need to better manage U.S.-China data flows and the use of high-risk Chinese technology inside the United States.

As I said a few minutes ago, I see the U.S. semiconductor export controls on China as having the hallmarks of an effective strategy to limit the flow of high-end semiconductors and semiconductor manufacturing equipment to China. But having an effective strategy to control the export of semiconductors and certain semiconductor manufacturing equipment to China is different from having an effective export controls strategy with respect to China as a whole. The strategic goal of U.S. export controls on China, after all, is not simply to maintain the U.S. advantage in one specific technology, but rather to maintain a significant military and technological edge over Beijing. The U.S. and our allies need to do across a range of critical technologies what we have now done with respect to semiconductors: identify technological chokepoints, and then leverage those chokepoints to slow China's development across a range of critical technologies.

The first step towards a comprehensive strategy for U.S. export controls on China is to develop a more fulsome and generally agreed list of the technologies that the U.S. should work to control, given our strategic objectives. I generally agree that when it comes to export controls the U.S. should, in the words of U.S. National Security Advisor Jake Sullivan, seek to build a high fence around a small yard. But we still need to reach a domestic consensus and an agreement with our allies and partners about the specific technologies and sectors that should be kept inside that fence.

Fortunately, the U.S. government already maintains a list of critical and emerging technologies that export control policymakers should consider as the basis for such a list: The Office of Science and Technology Policy's (OSTP) "Critical and Emerging Technologies List." [11] The most recent update to this list, which OSTP released in February 2024, contains 18 technologies: including advanced computing, AI, autonomous systems and robotics, semiconductors, and advanced materials, among others. This list reflects both a consensus among the U.S. Executive Branch about the technologies of greatest concern, and includes a number of technologies where we have seen recent work with allies to increase multilateral export controls at least where there are clear military applications of a technology.

[11] White House Office of Science and Technology Policy, "Critical and Emerging Technologies List Update," Feb. 2024, p. 2, https://www.whitehouse.gov/ostp/news-updates/2024/02/12/white-house-office-of-science-and-technology-policy-releases-updated-critical-and-emerging-technologies-list/.

In my view the U.S. government should work with allies and partners to identify potential chokepoints across the range of technologies on the OSTP Critical and Emerging Technologies list and evaluate the ones where export controls could play an important role in maintaining America's edge. Then, as OSTP periodically updates the list over time, export control policymakers should similarly update the focus of technology-related export controls. Developing effective export control strategies across this range of technologies will, of course, require additional resources, and I would urge Congress to expand resources for the Bureau of Industry and Security and other relevant export control agencies. Given that most export controls need to be multilateral to be effective, and considering the time and effort it usually takes to convince allies and partners to join in imposing multilateral controls, I second a recommendation that my co-panelist Kevin Wolf has made in his written testimony that the U.S. government appoint a senior-level diplomatic envoy tasked with building multilateral support for strong export controls.

But I think that an export control focus limited to critical and emerging technologies would be too narrow. As I said earlier, in my view the most effective way to deter China from engaging in a military conflict with one of its neighbors is to maintain a situation in which Beijing assesses it would not readily prevail in such a conflict. Consequently, in my view a comprehensive U.S. export control strategy should focus on ways to degrade Chinese defense industrial base sectors key to China's military modernization program, such as China's aerospace sector, which continues to rely heavily on western components and expertise.

Historically, one of the major objections to expanding U.S. export controls on Chinese defense industrial base sectors such as aerospace is that the U.S. would be unlikely to convince allies to impose parallel controls, and, as a result, the U.S. would simply disadvantage U.S. aerospace firms relative to their western competitors while having limited impact on China's development. I certainly agree that in many cases unilateral U.S. controls on major Chinese defense industrial base sectors would impose significant costs on U.S. companies while having limited impact on Chinese advances.

However, the deepening ties between China's defense industrial base and Russia's defense industrial base may present the U.S. with a moment of diplomatic opportunity. Having recently returned from discussions in Europe, it clear that European policymakers are deeply disturbed by recent public revelations about the depth of Chinese support for Russia's defense industrial base. This potentially opens the door to multilateral export controls that could be used to weaken China's own defense industrial base. At the very least, it is worth serious diplomatic discussions with our allies to determine what scope there might be to do so.

High risk Chinese technology and data flows

This brings me to the third and final topic that I would like to discuss, the need to develop a framework for managing the risks the U.S. faces from certain data flows to China and from the use of certain high-risk Chinese technology in the U.S.

In recent years both Congress and the Executive Branch have taken multiple important steps to address the risks posed by specific high risk data flows to China and by specific high-risk Chinese technology in the United States. Just last month, for example, Congress passed legislation that will, if upheld by the courts, require Chinese company ByteDance to divest its ownership of social media company TikTok or impose a ban on the distribution of TikTok in app stores in the U.S. This law

will help ensure that China cannot use TikTok to either collect sensitive data about Americans or covertly influence U.S. public opinion, and is consistent with U.S. restrictions on foreign ownership of U.S. media that date back more than a century. Congress has directed many U.S. government agencies to stop using Chinese drones, given the risk that they could send data back to China, and is currently considering broader restrictions on Chinese drones. The Department of Homeland Security earlier this year published an advisory about the risks that U.S. critical infrastructure firms could face from using Chinese drones. The Coast Guard is currently working to limit the use of Chinese cargo cranes in U.S. ports, given the risk that they could be used to track sensitive cargo entering and departing American ports.

The FCC has over the past year or two restricted the use of certain Chinese-made security cameras in the United States. The Commerce Department in early March published an advance notice of proposed rulemaking indicating that it may develop a rule restricting the use of Chinese connected car technology in the United States, given the potential for cameras and other sensors on U.S. cars to send sensitive data to Beijing. In February President Biden signed an Executive Order (E.O. 14117) directing the Department of Justice to establish new rules regarding the export of certain high-risk, bulk data to China and other countries of concern. The CFIUS Committee has reported that it has required data localization measures as part of the CFIUS approval process. Last month, as part of the same bill that seeks to force ByteDance to divest TikTok, Congress also passed legislation that empowers the Federal Trade Commission to enforce a ban on data brokers sharing or selling personally identifiable sensitive data to companies in China, Russia, Iran, and North Korea.

Each of these actions, individually, is important to protect U.S. data and U.S. national security. The Congress should continue to consider appropriate legislation as specific new threats arise. But the variety of actions—and this list is only a subset of the actions taken in recent years—is intended to illustrate my view that over the long term the U.S. needs to move beyond a piecemeal approach to addressing discrete risks to an integrated, proactive approach.

China has long been able to gain access to sensitive U.S. data through at least four primary vectors:

- Beijing can buy it, for example by purchasing data from data brokers or buying U.S. and third country companies that have access to sensitive U.S. data.

- Beijing can get Americans to give data to them voluntarily, for example by using Chinese apps and software that collect it.

- Beijing can introduce backdoors and other vulnerabilities into software and hardware used in the United States to covertly collect it.

- Beijing can hack into U.S. IT systems and steal it.

What the U.S. needs is an integrated approach that would address each of these threat vectors comprehensively. In my view, this includes at least five major lines of work:

- A national data privacy law that would limit the collection, aggregation, and sale of Americans' personal data. This would not only restrict Chinese companies and fronts for

Chinese companies from purchasing U.S. personal data, it would also make it more difficult for Chinese hackers to get access to bulk personal data because there would be less such data to hack in the first place.

- Continued development of cybersecurity standards to ensure that companies that store sensitive data and that operate software in critical infrastructure sectors are better able to resist malicious hacking by China and other threats.

- Targeted measures to prohibit the sale or transfer of certain sensitive data to China, building on the ongoing process to implement E.O. 14117.

- Continued use of CFIUS to ensure that Chinese companies, and companies that might be subject to Chinese influence, are not able to purchase U.S. companies and then get access to the sensitive data that those companies hold.

- A systematic approach to identifying and mitigating the risks posed by high-risk Chinese software and hardware in the United States. For example, Congress could codify and expand the Department of Commerce's "ICTS rule" and direct the Department to develop a framework and workplan to systematically evaluate which Chinese technologies in the U.S. should be subject to different degrees of restriction.

Specific actions across these lines of work are beyond the scope of my testimony today. But I would urge the Commission to dedicate a significant piece of work to data and technology security and to provide systematic recommendations to Congress in this area.

Closing

I now want to offer a minute of closing remarks. I have testified before the Commission today regarding export controls on China and on the importance of managing the U.S.-China technological relationship. I believe that export controls can play a vital role in helping to maintain America's technological and strategic edge over China and in reducing China's military potential. But if the U.S. is to maintain its strategic and technological edge over China over the long run, export controls are less important than is fostering domestic investments and technological innovations here in America and across allied countries. We certainly can and should work to trip up Chinese development across key technologies and the development of China's defense industrial base. But if the U.S. and our allies want to stay ahead in the technological and geopolitical race that will define the next decade or more, we must foster our own technological innovation. After all, we can't use export controls to prevent China from obtaining a technology that China simply invents first. My final recommendation to the Commission is that even as the U.S. focuses on export controls, sanctions, and other technological restrictions, we focus even more on the role that America's own innovation and growth will play in staying ahead of our leading geopolitical rival.

With that, I welcome your questions.