JANUARY 18, 2024

TESTIMONY BEFORE THE U.S. SENATE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

Hearing on “National Security Challenges: Outpacing China in Emerging Technology”

U.S. Economic Security Strategy, Authorities, and Bureaucratic Capacity

BY

Emily Kilcrease

Senior Fellow and Director
Energy, Economics, and Security Program
Center for a New American Security

I. Summary of Testimony

Chairman Brown, Ranking Member Scott, and Members of the U.S. Senate Committee on Banking, Housing, and Urban Affairs, thank you for the opportunity to provide testimony. While I am currently employed by the Center for a New American Security (CNAS), I am providing testimony in my personal capacity.[1] The testimony draws from a large body of research that I have conducted at CNAS, as well as my prior experience serving the U.S. public as a proud civil servant in the U.S. Department of Commerce, the National Security Council, and the Office of the U.S. Trade Representative, including most recently serving as the Deputy Assistant U.S. Trade Representative for Investment.

At the request of the Committee, this testimony focuses on three economic security tools that the United States has or is considering establishing: export controls; screening of inbound foreign direct investment (FDI), as implemented by the Committee on Foreign Investment in the United States (CFIUS); and the possibility of new authorities related to outbound investment controls. Specific analysis and recommendations for enhancing the capacity and effectiveness of each of these economic security tools is included, with a focus on how these tools can be used to maintain a U.S. technological lead vis-à-vis China. The testimony focuses on issues of strengthening economic security strategy, authorities, and bureaucratic capacity, rather than advising on specific technologies that may be suitable for more or fewer controls. Given common issues across the programs and the acute need for stronger integration and coherence across the economic security toolkit, the testimony begins with cross-cutting recommendations.

A summary of recommendations for congressional consideration are as follows:

Cross-cutting issues in the economic security toolkit

- Direct the administration to develop an economic security strategy that defines a clear vision for bounding the economic relationship with China to address national security risks, including specific and measurable plans for the use of economic security programs to address national security risks;

- Establish and provide resources for strategic planning functions in the agencies responsible for managing economic security programs, including dedicated full-time staff for strategic planning;

- Promote stronger alignment on economic security with key international partners and allies, including through guidance on the types of formal or informal arrangements that can facilitate stronger collaboration and resources to support expanded international outreach efforts;

- Establish and provide resources for dedicated offices to evaluate the effectiveness of existing and proposed economic security policies; and

- Facilitate government access to diverse, unbiased sources of information and expertise, including from industry, the intelligence community, and independent analysts.

[1] This testimony reflects the personal views of the author alone. As a research and policy institution committed to the highest standards of organizational, intellectual, and personal integrity, the Center for a New American Security (CNAS) maintains strict intellectual independence and sole editorial direction and control over its ideas, projects, publications, events, and other research activities. CNAS does not take institutional positions on policy issues and the content of CNAS publications reflects the views of their authors alone. In keeping with its mission and values, CNAS does not engage in lobbying activity and complies fully with all applicable federal, state, and local laws. CNAS will not engage in any representational activities or advocacy on behalf of any entities or interests and, to the extent that the Center accepts funding from non-U.S. sources, its activities will be limited to bona fide scholastic, academic, and research-related activities, consistent with applicable federal law. The Center publicly acknowledges on its website annually all donors who contribute.

Export controls

- Increase the budget for the Bureau of Industry and Security to match its expanded national security and foreign policy mandate and to enable it to fulfill new responsibilities related to strategic planning, evaluation, and international outreach;
- Mandate regular reviews of the Commerce Control List;
- Assess the effectiveness of country-wide controls on commercial technology exports to China, including the impacts on U.S. competitiveness and the feasibility of securing support for such controls from key international partners;
- Mandate the evaluation of novel export controls, such as the foreign direct product rules; and
- Require a study on the feasibility of releasing additional export control data to the public.

Committee on Foreign Investment in the United States (CFIUS)

- Expand the CFIUS definition of "critical technologies" to include "critical technologies controlled for investment purposes," as defined by CFIUS and focused on emerging technologies; and
- Address high case volumes and potential mission creep by passing data security and data privacy legislation and conducting oversight on the use of mitigation agreements for transactions involving firms located in U.S. allied countries.

Outbound investment controls

- Codify and provide resources for a targeted set of outbound investment controls focused on transactions that may enable China's indigenous development of technologies relevant to U.S. national security interests;
- Require mandatory notifications of U.S. investments in China to enhance U.S. government insights into the scoping and administration of outbound investment controls;
- Prohibit U.S. investments into high-risk technologies or sectors in China; and
- Expand the Non-SDN Chinese Military-Industrial Complex program to prohibit all types of investments in listed entities.

II. Introduction

China is a foremost geopolitical challenge for the United States. As Secretary of State Anthony Blinken has stated "China is the only country with both the intent to reshape the international order and, increasingly, the economic, diplomatic, military, and technological power to do it."[1] Unlike prior eras of strategic competition, China is deeply integrated with the U.S. and global economies, creating new types of national security risks from China's potential to weaponize these economic ties. While strategists might have previously bet on economic entanglement leading to geopolitical stability, Russia's brutal invasion of Ukraine and the increasingly authoritarian bent of China under Xi Jinping have rightly shaken policymakers' reliance on this view. The urgent task for the United States now is to mitigate national security risks arising from the

economic relationship with China, prevent China from exploiting the open nature of the U.S. market, and anticipate future risks that may emerge due to the rapid, global advance of critical technologies.

Meeting the China challenge will require the U.S. government to prioritize economic security programs (i.e., programs that address the national security risks that can arise from economic activities), including expanding the legal authorities and resources available to these programs across the executive branch. In the post 9/11 period, the Department of the Treasury was transformed to address the threat of terrorism, leading to major changes in how the United States can target the illicit sources of finance.[2] The U.S. government is in a similar moment now, with the need to fundamentally rethink and reorient how economic security programs are implemented to address the full range of risks presented by China. Technology competition is at the core of the U.S.-China strategic competition, and the role of technologies in economic security should be central to a strengthened government capacity to counter the China challenge.

III. Cross-cutting Issues in the Economic Security Toolkit

Too often, economic security issues are dealt with in bureaucratic silos. Economic security strategy tends to be a greatest hits list of what the government is already doing and has always done, rather than setting an ambitious vision to guide the use of economic statecraft tools. Program implementers stay confined to their area of bureaucratic turf and, through no fault of their own, are often too consumed by the intense day-to-day demands of dealing with ongoing crises to advance longer term objectives. These dynamics do not bode well for the whole-of-government approach needed to transform the U.S.-China economic relationship to better serve U.S. strategic interests and advance democratic values.

Congress can act to remedy these negative dynamics, including through directing the executive branch to develop an economic security strategy; establishing and providing resources for strategic planning functions in the economic agencies, including through dedicated full-time staff; pushing for greater alignment of U.S. economic security strategies and policies with key international partners; strengthening the government's capacity to evaluate the effectiveness of economic security programs; and ensuring that economic security functions have access to a wide range of non-biased, technical information.

U.S. Economic Security Strategy

The United States needs an economic security strategy. The Department of Defense recently released a defense industrial base strategy, the Department of Commerce is reportedly set to release its own national security strategy, and the Department of the Treasury in 2021 released a sanctions strategy.[3] That each agency is developing and releasing its own strategies is emblematic of the larger problem: the United States does not have a holistic vision for how to utilize all of its economic tools in tandem to achieve an articulated end state in the economic and geopolitical relationship with China.[4]

Recent CNAS research put forth one framework for developing economic security strategies, including introduction of the concepts of economic domain ends, ways, and means:

- **"Ends** specify the desired end state between the U.S. economy, its partners' economies, and that of its adversary, and are derived from broader … strategic objectives….
- **Ways** are the various methods of applying economic pressure … including a range of coercive economic statecraft measures such as financial sanctions, technology export controls, and tariffs.
- **Means** are defined in terms of the United States' relative capacity in an area of strategic economic activity."[5]

While this economic domain ends, ways, and means construct was developed in the context of research on sanctioning China in the event of a conflict, it equally applies to managing the economic security relationship

today. The United States must set a clear vision for what a future economic relationship with China looks like, balancing the economic need for continued ties with the security need to de-risk certain areas of economic activity. This vision should be derived from the broader national security strategy and focus on addressing the risks to national security that can arise from economic activities.[6] It then needs to develop specific, measurable strategies for how it can use all tools of economic statecraft to achieve the desired end state. Statements from administration officials have planted the seeds for what a potential strategy could look like, but none yet provide a clear view on how the United States should define the economic relationship with China to address growing national security concerns.[7] This is a particularly important gap, as the range of sectors that are assessed to have national security implications continues to grow and now encompasses much broader swathes of ordinary commercial activity.

This testimony focuses on three areas within the economic security toolkit. However, the potential range of policies and programs that could be used to advance U.S. economic security objectives (i.e., economic domain ways) are much broader and include tools such as tariffs and trade policy, subsidies, and restrictions on the import of information technology goods and services. Government procurement can also be used to address economic security issues, and Congress is considering bipartisan legislation to address government contracting with Chinese biotechnology companies, in one example of where this may be relevant.[8] How these tools are used in tandem to promote U.S. technological leadership should be a core element of an economic security strategy.

Semiconductors can provide a useful case study in the need for more holistic strategies. The United States has taken proactive steps to maintain U.S. advantage in advanced chips, including through precedent-setting export controls on technologies China needs to make advanced chips, as well as a large push on industrial policy to support domestic chips production and research and development. So far, so good. However, the effect of these policies is to create a structural incentive for China to double down on investments in legacy chip production, and the United States is not prepared to address a surge in imports of Chinese legacy chips.[9] Export controls would likely be ineffective, simply because China already has the technology necessary to make such chips. Tariffs, import restrictions, government procurement policies, and outbound investment controls could all play a role in addressing the import problem, though whether they can slow China's global growth without harming U.S. economic interests remains unclear. A more deliberative process for setting economic security strategy should anticipate these sorts of unintended consequences to enable more nimble and effective U.S. response to shifting market dynamics, including those shifts that are caused by actions of the U.S. government itself.

An effective economic security strategy will require breaking down of bureaucratic siloes and a sharp focus on prioritization of issues. It will require working across all the economic agencies in the executive branch and across multiple committees of jurisdiction in Congress. As officials proceed with developing economic security strategy, they must remain laser focused on addressing the most pronounced gaps in the U.S. toolkit. In addition to continual updating of export controls and CFIUS, passing legislation to address problematic vacuums in U.S. authorities, such as those related to outbound investment and data security (discussed further in later sections of the testimony), are an important part of an effective economic security strategy.

Strategic Planning Functions[10]

The agencies responsible for managing economic security programs should establish strategic planning functions, which would continually assess how economic security tools could effectively be used in a range of potential future scenarios with strategic competitors, with a focus on China. While this sort of strategic planning function is well established in the military community, it is practically non-existent for the economic agencies. Yet, should a crisis or conflict with China break out, economic tools would almost certainly be part of the U.S. policy response. An economic domain strategic planning process can enhance U.S. readiness for

such scenarios, as well as enable the United State to consider the deployment of economic tools in support of longer-term deterrence objectives and in the ongoing strategic competition with China.

Economic domain strategic planning should be carried out at three levels.[11] First, the economic agencies must deepen their institutional capacity to engage in long-term strategic planning. Second, planning must be integrated with similar planning exercises in the defense community in support of an "integrated deterrence" objective that utilizes all instruments of national power.[12] Third, U.S. planning must be integrated with that of U.S. partners and allies, leveraging the core U.S. strategic advantage of alliances.[13] Each of these areas must be staffed by experts whose full-time job is strategic planning, to avoid falling into the familiar trap of pushing off long-term thinking in order to deal with the crisis of the day.

Alignment with International Partners and Allies

Economic security programs are maximally effective when the U.S. approach is aligned with that of its key allies and partners abroad. While unilateral controls may be effective in the short-term and in some cases may be necessary to spur action from partners and allies, the effectiveness of unilateral measures erodes over time. U.S. firms must vigorously compete to maintain their leading role in global technology value chains, and restrictions only on U.S. firms will ultimately lead to foreign firms backfilling U.S. technology exports to China.[14] A classic case in this regard is U.S. export controls on satellite technology. Europe did not implement similar controls and European firms were active in advancing China's satellite technology developments.[15] In these scenarios, the United States has the worst of both worlds—lost revenue and minimal impact on China's indigenous technology development.

Various experts have put forth proposals for structures to enhance alignment on economic security with international partners. A new multilateral export control regime, designed with strategic trade control objectives in mind, could complement the current Wassenaar Arrangement structure, which coordinates country-agnostic controls.[16] Broader agreements could be negotiated with partners that enhance coordination on a range of economic security tools, including export controls and investment security but also encompassing supply chain resiliency tools.[17] Or, efforts could focus on strengthening the ability of partners and allies to implement unilateral controls under their domestic authorities, providing needed flexibility when the United States seeks to form ad hoc coalitions, such as it did recently with the Netherlands and Japan on semiconductor manufacturing equipment export controls. Ultimately, the right approach will be the one that can secure broad buy-in from a range of industrialized and emerging economies. To date, key partners have expressed skepticism about the viability of new formalized regimes, though multiple efforts at strengthening cooperation are underway (e.g., coordination on export controls and investment screening in the U.S.-EU Trade and Technology Council).[18]

To meaningfully advance international alignment, the United States must work with allies to address divergences in their strategic assessments of the threat presented by China, their legal frameworks to impose new controls, and their capacity to implement and enforce more robust economic security programs. Some progress has been made in strategic-level alignment, including at the G7, which issued an important leaders' statement on economic security and resiliency this past year.[19] While the views of many partners toward China are hardening, not least because of China's continued support of Russia's invasion of Ukraine, there remain important differences in their views on how hard and fast to pursue economic de-risking with China.[20] Divergent views on the threat posed by China will necessarily complicate efforts to align the development and use of economic security tools to address this threat.

U.S. partners and allies also tend not to have the same broad and flexible economic security programs that the United States enjoys. On export controls, the legal authorities of most partners and allies are limited to implementing the export controls agreed in the multilateral export control regime processes and they do not have easily available ways to impose unilateral controls.[21] FDI screening mechanisms vary, and while many

countries now have such mechanisms, their legal scope and maturity vary considerably. Very few partners and allies have outbound investment screening, with most U.S. partners and allies expressing some skepticism about the need for such authorities and waiting for the United States to act first before deciding whether to implement their own outbound investment programs. Further, international capacity to implement economic security programs lags that of the United States, with partners and allies tending to have smaller staff and more limited intelligence capabilities. These dynamics mean that the United States must prioritize outreach and technical assistance to partners and allies, as U.S. support and leadership can play a critical role in strengthening the economic security efforts of U.S. partners and allies.

Congress could promote stronger international alignment by pushing the administration to prioritize economic security issues in its diplomatic efforts with international partners, including important technology players in Europe and Asia. It can provide clear guidance on the types of formal institutions or agreements that the United States should seek to establish, while also setting realistic interim goals on strengthening alignment while such institutions or agreements are being considered by international partners. Funding the international coordination functions of the economic security agencies will be critical, as well as ensuring that the State Department political and economic officers have training in economic security issues and a mandate to prioritize U.S. economic security objectives in their engagements with foreign counterparts.

Evaluation

Economic security tools are being used at an unprecedented scale and for a range of novel policy purposes. Export controls, for example, have evolved from a limited tool designed to prevent accumulation of weapons into one of the United States' favored policy responses to address a broad range of national security and foreign policy objectives.[22] While the use of economic security tools is justified on national security grounds, policymakers must not forget that imposition of economic restrictions come with economic costs. Economic restrictions, if effective, shut off market access to one of the world's most consequential economies, which has for decades been a driver of scale and growth for U.S. technology companies. As the range of economic security policies continues to grow, the U.S. government must have a way to assess the cost and effectiveness of these measures, including their long-term impact on U.S. technological competitiveness.

Currently, the evaluation function for economic security policies is sorely under-resourced. While the Department of the Treasury has established an office to assess the economic impacts of its sanctions programs, no comparable office exists for other economic security tools. Congress could consider establishing new offices within the Departments of Commerce and the Treasury to evaluate the effectiveness of export controls and investment security programs, while also assessing the impact of these programs on overall U.S. competitiveness. The evaluation of these offices should be used to inform the development of new economic security measures and the updating of existing ones. In cases where a measure may have high cost but is necessary nonetheless for national security reasons, these evaluations can inform how the government might use other policy tools to mitigate any impacts on U.S. competitiveness.

Access to Information and Expertise

Effective implementation of economic security programs depends on access to diverse, unbiased sources of information and expertise. These programs must have deep knowledge in legal and regulatory issues, market issues, critical technologies, China's economic and technology landscape, and U.S. technological capabilities. Specialized skills, such as Mandarin language skills or deep technological expertise, are often in short supply within the government. While the agencies should prioritize hiring staff who possess these types of expertise, in reality the scope of expertise needed will always outpace the government's ability to hire, particularly when considering the fast pace of technological development in the commercial space. The economic agencies will need to leverage a wide range of sources of information and expertise, including:

- **Industry**: Industry often has the most up-to-date and detailed information on technology products, simply because it is their engineers who develop these products. Regular engagement with industry can help government policies keep pace with commercial developments, while also alerting the government to unintended consequences of specific policies. At the same time, an over-reliance on industry sources should be avoided, as industry will have an inherent bias in its perspective.

- **Intelligence**: The intelligence community must provide robust support to economic security functions. Ways of achieving this vary. In the CFIUS process, the Office of the Director of National Intelligence (ODNI) provides coordinated intelligence assessments for each transaction under review. For sanctions, Treasury has its own intelligence capabilities through TFI. For export controls, Commerce has an analytic office that provides support for enforcement purposes.

- **Independent analysts**: Independent, third-party organizations, such as think tanks, federally funded research and development centers, academia, and business intelligence services, can also act as sources of unbiased technical and strategic information for economic security programs.[23]

Congress could utilize its oversight functions to ensure that the economic security agencies are fully utilizing these sources of information. While not endorsing any particular proposal for ensuring more robust intelligence support for the export control programs, Congress could focus on whether the growing national security role of the Department of Commerce has sufficient support from the intelligence community. This should include intelligence support for export control licensing decisions and development of new export control policies, in addition to intelligence support for enforcement efforts, and should include capabilities to conduct Chinese-language, all-source intelligence analysis. Congress might also consider whether the agencies have sufficient resources to subscribe to business intelligence platforms or commission third-party studies, if doing so would support their overall missions.

IV. Export Controls

Export controls regulate the export, re-export, and in-country transfer of commodities, software, technologies, and, occasionally, services to specific destinations, end users, and end uses to achieve U.S. national security and foreign policy objectives.[24] The classic post–Cold War objectives of export controls were to regulate bespoke military and dual-use items (i.e., items with both military and commercial applications) that had some identifiable relationship to the development, production, or use of either weapons of mass destruction or conventional weapons.[25] With the export controls imposed against Russia in early 2022 and against China in late 2022, the U.S. government has expanded the scope of export controls to address broader strategic objectives regarding otherwise exclusively commercial items that nonetheless are of importance to the industrial bases of Russia and China.[26]

Dual-use export controls, which are the subject of this testimony, are governed by the Export Control Reform Act of 2018 (ECRA). ECRA provides broad authority for the United States to impose unilateral or multilateral controls to address a range of national security and foreign policy objectives, including those related to combatting weapons proliferation and terrorism, preserving the military superiority of the United States, strengthening the U.S. defense industrial base, protecting human rights and democracy, and facilitating military interoperability with allies.[27] Dual-use export controls are administered by the Department of Commerce, in close coordination with the Departments of Defense, Energy, and State.[28]

While Commerce and the export control agencies have a strong legal framework to implement controls for a broad range of national security and foreign policy objectives, their ability to do so may be hampered by under-resourcing, as well as a current lack of capacity to regularly evaluate the effectiveness of existing and proposed controls. The issues of resourcing and evaluation are further stressed by the greater role that export

controls are playing in U.S. national security and foreign policy, including the implementation of new and innovative types of export controls, the long-term effectiveness of which has not yet been proven.

Resources for an Expanded National Security and Foreign Policy Mandate

Export controls now play a leading role in U.S. foreign policy, not just in the China context but also as part of the sanctioning effort toward Russia and bolstering human rights, among other objectives.[29] As new and continually more novel types of export controls continue to be implemented, there is an acute need to ensure that Commerce has the corresponding increase in resources to monitor and enforce its new controls. Secretary of Commerce Gina Raimondo has urged Congress to invest in export controls, stating that the Bureau of Industry and Security (BIS), the agency within Commerce that administers export controls, has the same budget it did a decade ago (that is, before the Russian invasion of Ukraine and before the rise of Xi Jinping).[30] As one export control official noted, "[w]e spend 100 percent of our time on Russia sanctions, another 100 percent on China and the other 100 percent on everything else."[31]

Examining the budget numbers for BIS provides another perspective on the question of resources. BIS's enacted budget in 2012 was $101 million (adjusted for inflation, this number would be approximately $133 million).[32] In 2023, the enacted budget was $191 million and the requested budget for 2024 is $222 million.[33] However, while resources may appear to be growing for BIS, a substantial portion of these increases have been driven by non-export control related activities, such as the implementation of new authorities related to regulating the imports of information and technology goods and services, as well as adjustments for inflation and mandated civilian pay increases.[34] This suggests that resources for the functions described in this testimony (strategy development, strategic planning with the interagency and international partners, evaluation of existing and proposed controls) remain a gap that Congress may want to address through further investment in BIS capacity in these areas. To date, these functions either do not exist or are under-resourced relative to the national security need. Additionally, established functions in export administration and export enforcement are likely not receiving sufficient investment, given growing demands. For example, the number of licensing applications has grown on average in recent years, with applications peaking near 40,000 in 2020 compared to annual averages closer to 24,000-31,000 in the 2014–2015 period.[35] Increased use of extraterritorial controls, discussed in more detail later, also increases the need for export control officers to be based overseas to conduct monitoring and enforcement activities.

Think tank analysis has proposed increased funding levels for particular BIS programs. CNAS AI researchers recommend $10 – 12 million in funding to implement an AI chip registry and random sampling program, both of which are intended to bolster technical methods of export controls enforcement.[36] The Center for Strategic and International Studies recommends approximately $45 million to modernize analytic and enforcement capabilities.[37] Importantly, these analyses recommend not just more money, but more money wisely spent. The fast-expanding scope of export controls and complex enforcement environments mean that simply scaling up existing processes are likely to be ineffective. Innovative technical approaches to enforcement, such as using on-chip governance mechanisms to track the deployment of advanced AI chips, should be part of Congress's considerations related to increased resources.[38]

Many recommendations in this testimony, including the review of the Commerce Control List, establishment of strategic planning and evaluation functions, international engagement, and public release of export control data, would all require resources, which Congress should assess.

Regular Review of the Commerce Control List

As the United States continues to expand the national security and foreign policy objectives for which it uses dual-use export controls, it must regularly review its control lists to ensure that it is capturing those technologies relevant for these expanded objectives. The Commerce Control List is the vehicle for listing and

controlling dual-use technologies, including the licensing policies for each listed technology.[39] It is questionable whether the Commerce Control List is reflective of today's high-priority, national security–relevant technologies, particularly with respect to emerging technologies. Regular and holistic reviews of the Commerce Control List could help ensure that it reflects the current state of technological competition with China, including in emerging technology areas that currently do not have high levels of controls (e.g., AI).

Congress could direct—and provide resources for—Commerce to conduct a top-to-bottom review of the Commerce Control List, report to Congress on the results, and provide a plan for updating controls based on this review within a set period. The review could include all items currently listed for any reason on the Commerce Control List, as well as examination of whether new controls should be implemented for those technologies that were identified in the list of critical and emerging technologies developed by the White House Office of Science and Technology Policy and the National Science and Technology Council.[40] Recent requirements to review the U.S. Munitions List can inform additional aspects of the suggested Commerce Control List review, including that it should consider interagency resources to implement existing and future controls, evolving technological and economic factors, and whether such technologies are available from other suppliers globally.[41] Congress could consider requiring regular reviews to ensure that there is continued attention and prioritization of list updates to keep pace with changes in the threat and technology landscapes.

Related to points made in the cross-cutting analysis of this testimony, reviewing the Commerce Control List will require Commerce to have access to a wide range of unbiased technical expertise. While Commerce should work companies to benefit from their technical and commercial knowledge, an industry-heavy approach to updating the Commerce Control List will be insufficient to meet current U.S. national security needs. Commerce will need to leverage expertise from other sources, including close coordination with the Departments of Defense, State, and Energy, as well as the intelligence community. Congress could require such interagency coordination and intelligence support as part of its direction to Commerce to conduct the list review. Additionally, Congress could consider specific funding for external analysts to conduct research in support of the list review. Regardless of the source of expertise, certain skills will be critical: Chinese language capabilities, industry and markets expertise, trade data analysis, engineering and technical knowhow, and expertise in China's indigenous technology development capabilities.

Country-Wide Controls in Response to Military-Civil Fusion

The United States has begun to implement country-wide controls on certain technologies in response to China's military-civil fusion strategies. Dual-use export controls have historically been implemented to prevent the flow of sensitive goods to military end uses or users while permitting the flow of goods to commercial purposes. However, China's military-civil fusion strategy complicates efforts to make clear distinctions between what is commercial and what is military. The merging of the civilian and military spheres is seen as a critical way by which China can leverage the whole of its economy in support of its military modernization goals, including through the development or acquisition of dual-use technologies such as semiconductors, AI, and quantum computing.[42]

The October 7 export controls on chips, AI, and supercomputing reflect a new U.S. approach for responding to China's military-civil fusion. These controls do not attempt to distinguish between military and commercial purposes. Instead, they establish a bright line test to prohibit the export of certain technologies to China based on how advanced a technology is and are applied for *all* users and purposes in China. The stark implication of this approach is to declare the further advancement of China in these technology areas to be a de facto national security risk, regardless of whether the advances are used for civilian or military purposes. As National Security Advisor Jake Sullivan noted, the new U.S. objective is to use export controls to maintain "as large a lead as possible" over China in those technology areas that are "force multipliers" for U.S. technological leadership.[43]

Congress has an important role to play in assessing whether this country-wide approach to controlling exports of dual-use technologies is effective. To date, certain October 7 controls have been complemented by similar controls from U.S. partners, namely controls on advanced semiconductor manufacturing equipment that were implemented by the Dutch and Japanese governments. However, many partners are skeptical of the new U.S. approach, and Congress should push the administration to prioritize further alignment on country-wide controls with key international partners. As with all controls, a more aggressive strategy of using country-wide controls will likely be unsustainable over time if not supported by like actions from other key producer nations.

Congress could push the administration to provide additional clarity and guidance on which sectors are suitable for country-wide controls. To date, semiconductors have been the focus of this approach, but the administration appears to be considering new controls in other areas, including cloud computing and quantum technologies.[44] International partners will need this type of clarity to understand the full breath of the administration's strategy, and additional assurances that the strategy will remain contained to a "small yard, high fence" philosophy, as the administration currently claims, will likely be necessary to secure their support for any future controls.[45]

Congress could encourage a consistent approach to using country-wide controls across the economic security tools. For example, the administration's executive order on outbound investment includes a prohibition on U.S. investments in Chinese companies involved "in the development of software that incorporates an AI system and is designed to be exclusively used for military, government intelligence, or mass-surveillance ends uses."[46] This very narrow scoping is unlikely to cover many AI systems, given that few if any AI systems are "exclusively used" for purely military ends. This type of measure, which will likely return a null set, appears to be inconsistent with a strategy designed to apply economy-wide controls on force multiplier technologies such as AI.

Evaluation of Novel Export Controls

While strengthening government capacity to assess the effectiveness of all export controls is essential, it is particularly critical to evaluate the use of novel export controls that are now being used in unprecedented ways, including to achieve new types of national security and foreign policy objectives. Foremost among these are the foreign direct product rules (FDPRs).

FDPRs are an oft-cited and oft-misunderstood tool. An FDPR allows the U.S. government to apply a control to a foreign-made product, if that foreign-made product is manufactured using U.S. technologies. U.S. technology need not be integrated into the foreign-made product for the FDPR to apply (controls related to integration of U.S. technology into a final good are addressed under a separate set of *de minimis* rules). Instead, the regulatory hook could simply be that a U.S. machine was made to manufacture a foreign good, even if that foreign good has absolutely no U.S. content integrated into it. The foreign-made item is subject to the export control so long as the foreign manufacturer continues to use the U.S. machine to produce its products. Each application of an FDPR is bespoke and designed for a specific scope of products and technologies. Thus, there is no one single FDPR, but several FDPRs, which can be found in section 734.9 of the Export Administration Regulations.[47] FDPRs are most effective when targeting manufacturing technologies in which the United State is dominant, namely semiconductor manufacturing, and will not work in other sectors if U.S. equipment is not similarly present in all global manufacturing facilities.

While FDPRs have existed in export control policy for decades, the tool took on a new dimension when a novel FDPR was imposed on Huawei in 2020.[48] Earlier, the U.S. government had placed Huawei on the Entity List in May 2019, but this restriction did not prohibit U.S. and foreign companies from selling most foreign-made commercial items to Huawei from outside the United States.[49] The 2020 Huawei rule used an FDPR to dramatically expand the scope of controls on the shipment of goods to Huawei, including on an

extraterritorial basis, leveraging the critical role of U.S. firms in the global semiconductor supply chains, specifically related to semiconductor manufacturing equipment (i.e., tooling) and electronic design automation (EDA) software. Virtually no chip made anywhere in the world can be produced without using some U.S. tooling or EDA software. The Huawei FDPR leveraged this dominant U.S. market position to prohibit the sale to Huawei of any chip made anywhere in the world, if the chip was made using U.S. tooling or EDA software. This drastically shut off the supply of chips to Huawei.[50] At the time, this application of the FDPR could be viewed as a one-off move to address concerns of the Trump administration with Huawei.

However, once a tool has been developed, governments tend to use it. In 2022, the United States implemented a set of far-reaching FDPRs as part of efforts to sanction Russia following its 2022 invasion of Ukraine.[51] The expanded use of FDPRs in this context was justified by the extraordinary nature of the crisis, with clear violations of international law requiring a strong response, ushering in the use of export controls as a sanctioning instrument. The United States reached for FDPRs yet again when imposing new controls on the export of advanced chips to China, as part of the aggressive controls released in October 2022 to stem China's advances in advanced chip production, AI, and supercomputing (the October 7 controls).[52] The use of FDPRs in the October 7 controls indicates that FDPRs will now be used as a matter of course by administrations of both political parties when addressing a range of foreign policy and national security concerns.

Yet, it is not clear that FDPRs are having their intended effect. When faced with the controls, Huawei doubled down on investments in its own chip capacity, with some degree of success as the late 2023 release of the Huawei Mate 60 Pro phone using a Hi-Silicon designed, SMIC-fabricated 7 nanometer chip shows.[53] Russia continues to have access to a disconcerting level of Western chips.[54] FDPRs, which are inherently extraterritorial, are also controversial with key allies, who tend to chafe at the application of U.S. law in their jurisdictions. FDPRs are very difficult to investigate and enforce, as they involve commercial items that are made outside the United States, without any U.S.-origin content, manufactured by non-U.S. companies and sold to other non-U.S. companies. Further, FDPRs will eventually lose their bite if foreign firms begin to design out U.S. tooling to increase their autonomy to operate in a global chips marketplace without the constraint of U.S.-imposed controls. FDPRs are only relevant so long as the foreign firm continues to use the U.S. tooling, and eventually foreign fabs (including those outside of China) may replace U.S. tooling with that available from Dutch and Japanese competitors, thus rendering ineffective the future use of FDPRs.

As Congress considers strengthening the evaluation capacity of Commerce, it could prioritize the evaluation of these types of novel export controls. There is a keen need to understand how companies are responding to FDPR constraints. For Chinese firms, this should include an assessment of whether they are able to illicitly access U.S. chips in contravention of the FDPRs. It should also assess the extent to which FDPRs have spurred indigenous innovation in China. As importantly, the effect of extraterritorial measures on U.S. competitiveness, including the prospect of non-China foreign fabs designing out U.S. tooling, should be examined. Designing out of U.S. tooling is a completely legal and foreseeable consequence of extended extraterritorial measures. This means that the economic impact for U.S. tooling firms could be significant, as they lose access to a broader range of global markets, not just the China market.[55] Designing out may take years to occur, given the complexity of the technology involved, and thus U.S. assessments of potential impact should encompass both short- and long-term projections.

Export Control Data for External Researchers

External evaluation of the effectiveness of export controls is hampered by the lack of publicly available data, specifically data the enables one to analyze exports based on their export control classification. Researchers can approximate the flow of controlled goods using tariff codes, but tariff codes and export control classifications do not neatly align. This significantly complicates efforts to judge the effectiveness of current controls and to project the impact of new controls under consideration.

Exporters are required to report exports of certain items to the U.S. government, including all exports to China of items listed on the Commerce Control List.[56] This reported data on exports is analyzed by BIS and may inform its internal deliberations. However, very little information is released publicly, even in aggregated form. Congress could direct Commerce to study the feasibility of releasing substantially more export data publicly, including data that would enable external evaluation of trade flows by export control classification category. Data releases could be structured or aggregated in a manner that protects business confidential information.

V. Committee on Foreign Investment in the United States (CFIUS)[57]

The United States has a well-established legal framework for screening certain foreign investments into U.S. businesses to address the national security risks that may arise from such transactions. These authorities are implemented by CFIUS, an interagency body chaired by the Secretary of the Treasury.[58] CFIUS has broad authority to respond to national security risks arising from foreign investments covered by its jurisdiction (*i.e.*, covered transactions.)[59] "It can do this through the negotiation—or in some cases, imposition—of terms on a transaction to mitigate identified national security risks. Where mitigation cannot overcome the national security concerns, CFIUS may recommend that the president suspend or prohibit the covered transaction. The CFIUS program, implemented on a day-to-day basis by hundreds of civil servants working across the executive branch and subject to high levels of political accountability, is generally functioning well."[60]

In 2018, Congress provided substantial updates to the CFIUS process through the Foreign Risk Review Modernization Act of 2018 (FIRRMA), which passed in tandem with ECRA. FIRRMA updates included: an expansion of CFIUS jurisdiction to review new types of non-controlling investment transactions and greenfield real estate transactions; strengthening of mitigation and enforcement capabilities; streamlined filing requirements for certain transactions; and incentives for international partners to align their FDI screening mechanisms with CFIUS. Importantly, the FIRRMA reforms came with a corresponding increase in resources and staff for Treasury and other CFIUS agencies to implement their expanded responsibilities. Congressional attention to the question of resources has been critical to ensure that CFIUS can effectively implement FIRRMA and respond to a dynamic threat environment.

Post-FIRRMA, CFIUS generally has the legal authorities and institutional capacity it needs to address national security risks associated with foreign investments. However, Congress may wish to consider a series of targeted updates to address evolving threats related to technology competition with China. Specifically, Congress may wish to expand the CFIUS definition of critical technologies to strengthen CFIUS jurisdiction over transactions involving emerging technologies. It could also consider a stronger oversight role in addressing high case volumes and potential mission creep of CFIUS, which may be over-burdening the CFIUS process and diverting resources from technology-related transactions.

Expansion of Critical Technology Definition

CFIUS has traditionally defined "critical technology" through reference to the export control authorities, rather than developing its own lists of sensitive technologies. For a technology to be considered a critical technology for CFIUS purposes, the technology must have been identified and listed by the export controls agencies on one of the U.S. export control lists (*e.g.*, the U.S. Munitions List or the Commerce Control List).[61] Prior to FIRRMA, this definitional issue had little practical impact. CFIUS had—and continues to have—full jurisdiction to review any transaction that conveys "control," as defined in FIRRMA, over the U.S. business to the foreign investor, regardless of whether the U.S. business engages in critical technology or not.[62] "Under FIRRMA, however, the definition of critical technology took on heightened importance in two ways. First, new CFIUS jurisdiction over covered investments (i.e., investments that conveyed important benefits, short of full control, to the foreign investor) was limited to only certain types of U.S. businesses, including those

that engaged in critical technology as defined through reference to export control authorities. Second, the new FIRRMA authorities to mandate notifications of certain transactions to CFIUS also hinged on the definition of critical technology. These changes gave new importance to the linkage between export control authorities and CFIUS."[63]

Consistency between CFIUS and export controls is generally a best practice, as it enhances policy coherence across the various authorities and facilitates private sector compliance. However, in certain cases, risks that arise from an investment transaction may differ meaningfully from risks arising from an export. Export risks relate to an adversary gaining new access to a technology that has national security relevance. In contrast, investment risks may include a much broader range of potential risk scenarios, including those related to the foreign investor's access to privileged information about a U.S. business or the ability to influence decisions of that business.

Artificial intelligence is a useful case study for assessing the different types of risks arising from exports and investment transactions. Frontier AI systems (i.e., often defined as general-purpose systems at the frontier of AI research and development) are showing increasing capabilities to mimic human cognitive abilities and learn new skills through ingesting and analyzing massive amounts of data. Though these systems retain many rough edges, there are already indications of potential national security harms that could arise from misuse, including the enabling of cyberattacks, spreading disinformation, conducting weapons testing, or developing novel toxins.[64] Many experts are concerned that these same capabilities could lead to catastrophic outcomes, either via accident or deliberate misuse.[65] How frontier AI systems are developed to guard against these risks is inherently a matter of governance, and governance is deeply reliant on the interests, values, and ethics of the individuals in charge of AI companies. CFIUS should have broad jurisdiction to review how foreign investors may influence these governance dynamics, regardless of whether the U.S. business "produces, designs, tests, manufactures, fabricates, or develops" technology that is currently subject to U.S. export controls (i.e., whether the U.S. business meets the FIRRMA definition of engaging in critical technologies).[66] Currently, AI export controls are very limited and largely confined to AI chips. AI companies (either frontier AI labs or other start-ups that leverage AI systems built by these labs) do not always make their own chips and thus would likely not be caught by current CFIUS jurisdiction. Enabling CFIUS to identify and remedy these sorts of scenarios can address jurisdictional gaps and allow for more robust oversight into the range of risks that foreign investments into U.S. emerging technology ecosystems can present.

Specifically, Congress could expand the definition of "critical technologies" in FIRRMA to include a new category of "technologies controlled for investment purposes." This new category would be additional to the existing definitions. Congress could require CFIUS to issue regulations within one year to identify those technologies that would be defined as "technologies controlled for investment purposes" and direct them to consider all technologies listed as critical and emerging technologies by the White House Office of Science and Technology Policy.[67] Finally, Congress could provide guidance to CFIUS that for transactions involving "technologies controlled for investment purposes," CFIUS should consider all national security risks that may arise from the foreign investor's involvement in the transaction, including how the foreign investor may shape the use and deployment of the technology. The new authorities should be narrowly targeted at investments from competitor nations, to avoid chilling beneficial investment from U.S. partners and allies.

High Case Volumes and Potential for Mission Creep

CFIUS is reviewing historically high numbers of transactions. In 2022, the most recent year for which Treasury has reported data, CFIUS reviewed 154 short-form declarations and 286 notices.[68] This is roughly double the number of transactions that CFIUS reviewed pre-FIRRMA. CFIUS is also negotiating or imposing mitigation terms on transactions at historically high levels, with 41 mitigation agreements for transactions filed in 2022—the highest amount in the post-FIRRMA period.[69] These increasing case volumes require continued congressional attention to ensure that CFIUS has the budget and staffing in all CFIUS

agencies to carry out CFIUS responsibilities. This is essential both to address urgent national security risks, as well as to ensure that beneficial investments can clear the CFIUS process in a predictable and expeditious manner, consistent with the U.S. open investment policy.

The high case volumes are driven in part by the increased expansion of jurisdiction under FIRRMA, but they are also a result of CFIUS stepping in to fill gaps in other authorities. The most pronounced area in which CFIUS is filling a policy void is related to data privacy and data security. In the absence of national legislation to provide robust data privacy protections for individuals and to regulate the transfers of sensitive bulk data overseas, CFIUS is often left to use its mitigation authorities to address data risks that appear in the context of a foreign investment simply because it is the only authority available to do so. CFIUS is intended to be a tool of last resort, and it is not designed to address all risks that may be present in the U.S. economy. Instead, when it comes to data privacy and security, CFIUS "has become a tool of convenience to impose a patchwork of protections for sensitive data held by companies that just so happen to be receiving a foreign investment."[70]

As noted in prior testimony, "Congress can help by passing comprehensive data privacy and data security legislation. Data privacy objectives should include giving individuals greater control over what data is collected about them online and how that information is sold or used. Data security objectives should address the national security concerns that can arise from the bulk transfer of sensitive data to a foreign adversary. Data privacy and data security have overlapping objectives and stronger data privacy will inherently reduce data security risks through minimization of the personal data on the open market. Data privacy and data security legislation is important in its own right but will also help return CFIUS to its intended purposes of addressing foreign investment risks rather than dealing with data risks writ large."[71]

CFIUS's assessment of third-party risks represent another area in which CFIUS may be over-extended. Third-party risks arise when a foreign investor's relationships with competitor nations, rather than the foreign investor itself, that raise concerns. For example, CFIUS may be concerned if a European company with extensive business operations in China is acquiring a sensitive U.S. business, as the technology of the U.S. business could indirectly leak to China post-investment. The high level of mitigation agreements in 2022, paired with an overall decline in Chinese investment in the United States, may be an indicator that mitigation agreements are increasingly being used for third-party risk.[72] While CFIUS has clear authority to address such concerns, it would be far more effective if U.S. partners and allies strengthened their own economic security toolkits to address these concerns directly in their own jurisdictions. While the Departments of Treasury and State have made admirable strides in encouraging FDI screening in partner and allied countries, many of these mechanisms remain less mature than the CFIUS and coordination with the United States on assessing investment risks varies significantly by country.

Congress could remedy these issues by providing robust resources to the investment security international outreach functions in Treasury and State. Additionally, Congress has an important oversight role to ensure that aggressive CFIUS mitigation of investments from U.S. partners and allies is not chilling the U.S. investment climate or straining U.S. alliances. Congress could institute "a new requirement for CFIUS to assess and report to Congress on the impact of the CFIUS process on foreign investment flows from allies and partners. This should include assessment of whether these flows have been negatively impacted by FIRRMA's expansion of CFIUS jurisdiction and whether FIRRMA's tools to address this, including the exempted foreign state program and the declaration process, are being effectively utilized. The reporting requirement should also address the impact of mitigation agreements on the investments of allies and partners, with the aim of ensuring that these mitigation agreements are genuinely focused on risks arising from the transaction and attributable to the foreign investor, rather than broader systemic risks."[73] Congress may also want to consider strengthening the role of the Office of Legal Counsel (OLC) within the CFIUS process, to guard against potential mission creep and ensure that all CFIUS decisions could withstand external or judicial review.[74]

VI. Outbound Investment Controls[75]

U.S. policymakers are currently debating whether and how to regulate U.S. investments in China (i.e., outbound investment). The administration has released an executive order, with an accompanying advanced notice of proposed rulemaking (ANPRM), outlining a targeted proposal to mandate notifications of—and in come cases, prohibit—certain U.S. investments into China's AI, semiconductor, and quantum technology ecosystems.[76] Congress has considered a range of proposals, with current efforts in the Senate coalescing around a mandatory notification program.[77] Debate remains ongoing in the House of Representatives, with the House Financial Services Committee advancing legislation that leans more heavily on traditional sanctions tools to address concerns with outbound investment.[78] The House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party, in its recent report on the U.S.-China economic relationship, has recommended new authorities to implement a sectoral approach to regulating outbound investment.[79]

The following analysis and recommendations draw from joint work conducted by the author and Sarah Bauerle Danzman, including the report *Sand in the Silicon: Designing an Outbound Investment Mechanism* published jointly by the Atlantic Council and CNAS.[80] Highlights of *Sand in the Silicon* are provided here, and additional detail and analysis can be found in the report. Dr. Danzman testified before the Committee on September 29, 2022 in the hearing titled "Examining Outbound Investment."

The National Security Case for Regulating Outbound Investment

Certain U.S. investments in China present national security risks that are not addressed by existing U.S. authorities. U.S. firms and investors may, in some cases, be supporting the development of critical technologies in China that have important national security applications. These include investments related to chips, AI, or other technologies that can accelerate advances in Chinese military capabilities.[81] Just as U.S. law and policy have long recognized that the export of certain technologies can be counter to U.S. security interests, so too can certain overseas investments if such investments are contributing to increasing military capabilities of competitor nations. While officials have raised a wide range of concerns related to U.S. investment in China, including related to human rights, offshoring of U.S. jobs, and financial stability, outbound investment controls would not be appropriate in each of these areas.[82] The goal of an outbound investment program is not to impose broad capital controls, but to instead address the specific transactions through which critical industrial knowhow may transfer to China and to plug a specific gap that export controls cannot fill in the technology competition with China.

Outbound investment controls can be best thought of as a complement to U.S. export controls, filling a gap related to non-technical expertise that export controls are ill suited to capture. Export controls address part of the national security risk associated with outbound investments, namely the risk that investments may involve the transfer of sensitive U.S. technologies. However, export controls do not cover the full range of risks associated with outbound investment transactions, particularly those that arise from the transfer of management expertise or other non-technical industrial knowhow. For example, one can consider the broad range of skills and expertise needed to establish and operate a semiconductor fabrication facility that can produce high-quality chips at scale and on commercially competitive terms. Technical knowledge and technology innovation will be critical to this business, and export controls can address this aspect of potential risk associated with U.S. investments into China-based facilities. But, the operators of these facilities will also need to manage complex supply chains, maintain a skilled workforce, and develop commercial strategies for succeeding in a cutthroat global marketplace. Few companies today can master these complex operational and management requirements. This type of management expertise is one example of the non-technology related benefits that can flow along with an outbound investment that are not, and never would be, suitable to capture under export control authorities.

Designing New Outbound Investment Controls

Addressing national security risks associated with U.S. investments in China will require a carefully calibrated approach. Overarching principles guiding the development of future outbound investment tools should include that such tools should be:

- targeted at transactions of highest national security risk;
- clearly defined and understandable to private-sector entities, who will be responsible for the first line of compliance;
- non-duplicative of and consistent with existing tools, including export controls;
- scoped proportionately to the administrative capacity available to effectively administer a new mechanism; and
- designed to enable meaningful conversations with allies about adopting similar regimes, including the need to limit extraterritorial application of U.S. authorities.[83]

Consistent with these broad principles, the United States should focus on U.S. investments that: 1) convey management expertise or other industrial knowhow along with the investment; 2) are made into critical technology sectors in China; and 3) may advance the indigenous development of China's technology capabilities in areas relevant to national security.

Given the complexity of the investment environment in China, the United States will need a multi-pronged approach to adequately address the national security risks associated with certain U.S. investments in China. This should include:

- **Mandatory notification requirements**: The U.S. government does not have full visibility into the entire scope of investment transactions being made by U.S. investors in China. Existing data sources are often too aggregated or incomplete, providing little information on the critical technologies involved in investment transactions. Recent Chinese efforts to crack down on Western due diligence firms further complicate attempts to understand the investment environment. Mandatory requirements to notify a defined scope of transactions to the U.S. government, subject to strict confidentiality requirements, is an important tool that can inform the design and administration of an effective outbound investment regime. Both the U.S. Senate and the administration have put forth proposals for notification requirements, though neither is yet in effect.[84]

- **Prohibitions of investments into high-risk technologies or sectors**: The U.S. government should prohibit U.S. investments in sectors in China that have clear military relevance. The government could establish a prohibition on U.S. investments in any Chinese firm that produces, designs, tests, manufactures, fabricates, or develops any technology that meets the technical specification of a technology that is subject to a U.S. arms embargo with respect to China, which would capture items on the U.S. Munitions List as well as space and military items listed on the Commerce Control List.[85] Additionally, prohibitions could be considered for investments into Chinese firms making other technologies subject to high levels of export controls, such as advanced semiconductors that meet the technical thresholds set in the October 7 controls. These sorts of prohibitions have an inherent logic, as U.S. persons should not be able to financially support Chinese indigenous development of the exact technologies that are prohibited from export to China.

- **Entity-based restrictions**: The U.S. government should establish authorities to prohibit U.S. investments into particular Chinese entities, as a complement to a sector-based notification and prohibition requirements. This allows for stronger action with respect to specific entities that the U.S. government may identify as acting against U.S. national security or foreign policy interests. The government has certain entity-based investment restrictions under the Chinese Military-Industrial

Complex (non-SDN CMIC) program. However, this authority is limited to the purchase or sale of publicly listed companies. Expansion of this program to include all types of investment transactions, as well as authorizing the designation of companies that are supporting Chinese indigenous development of national security technologies, can strengthen overall efforts to address investment-related national security risks. While certain policymakers have advocated for the use of full blocking sanctions to address outbound concerns, the use of this more severe form of sanction is highly escalatory and can exacerbate dedollarization risks.[86] Premature use of full blocking sanctions will erode the power of the U.S. sanctions threat over China, which should be preserved for moments of acute crisis or conflict.[87]

- **End use restrictions**: The U.S. government should establish investment restrictions based on the intended end use of the technology of the invested Chinese company. For example, U.S. investments should not be permitted into Chinese companies developing technologies with military, intelligence, or mass surveillance end uses. End use restrictions can complement sectoral and entity-based restrictions, mirroring a similar construct in export controls, which include list-based, end use, and end user controls. Crafting end use controls, however, must reflect the inherently dual-use nature of many technologies that are at the heart of the U.S.-China competition. For example, the administration's executive order includes an end use rule related to the development of AI systems for exclusively military end use, which is an unhelpfully narrow scope and would miss key AI labs in China, as frontier models today are inherently dual use.[88]

Congress has an essential role in establishing any new outbound investment authorities. While substantively the administration's executive order generally aligns with the recommendations of this testimony, implementing these authorities under executive action is not optimal over the longer term. Congress should act to codify and shape new outbound investment authorities, as well as to appropriate necessary resources and to conduct rigorous oversight to ensure that the authorities are being implemented effectively to advance U.S. national security interests.

VII. Conclusion

The United States faces a new era of strategic competition with China, one that presents challenges fundamentally different than prior eras due to China's essential role in the global economy. U.S. policy must account for objectives in tension with one another, including the need to de-risk economic ties that present pronounced national security risks while maintaining those ties that are in the U.S. strategic interest and ensuring the stability of the global economy. Navigating these difficult waters requires a clear strategic vision, bureaucratic orientation toward the China challenge, and a clear-eyed assessment of whether current U.S. policies are working. This analysis and recommendations in this testimony are intended to further these goals.

VIII. Additional Analysis

The following reports and analysis are cited in this testimony and are highlighted here for the convenience of the Committee in its future work.

Sarah Bauerle Danzman and Emily Kilcrease, "The Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail," *Foreign Affairs*, December 30, 2022, https://www.foreignaffairs.com/united-states/illusion-controls.

Sarah Bauerle Danzman and Emily Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism* (The Atlantic Council, September 14, 2022), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sand-in-the-silicon-designing-an-outbound-investment-controls-mechanism.

Emily Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China* (Washington, D.C.:, Center for a New American Security, December 1, 2023), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/EES-No-Winners_Final-1.pdf.

Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators: Hearing Before the U.S.-China Economic and Security Review Commission (2022) (statement of Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program, CNAS), https://www.cnas.org/publications/congressional-testimony/challenging-chinas-trade-practices.

The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission, 118th Cong. (2023) (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), https://www.uscc.gov/sites/default/files/2023-04/Emily_Kilcrease_Testimony.pdf.

Emily Kilcrease, Jasper Helder, and Kevin Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council* (January 14, 2022), www.cnas.org/publications/commentary/public-commentskilcreaseus-and-eu-export-control-cooperation-under-the-us-eu-trade-and-technology-council.

Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China* (Washington, D.C.:, Center for a New American Security, March 2, 2023), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmic-and-entity-list-designations-on-china.

Emily Kilcrease, Tim Fist, Sarah Bauerle Danzman, Ngor Luong, and Emily Weinstein, *Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of* Concern (September 29, 2023), https://www.cnas.org/publications/commentary/comments-on-provisions-pertaining-to-u-s-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern.

Emily Kilcrease, *Noteworthy: The New Russia Export Controls* (Washington, D.C.: Center for a New American Security, March 7, 2022), https://www.cnas.org/press/press-note/noteworthy-the-new-russia-export-controls

Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," War on the Rocks, Metamorphic Media, January 6, 2023, https://warontherocks.com/2023/01/how-to-win-friends-and-choke-chinas-chip-supply/.

Emily S. Weinstein and Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies* (Center for Security and Emerging Technologies, February 2023), https://cset.georgetown.edu/publication/u-s-outbound-investment-into-chinese-ai-companies/.

Stacie Pettyjohn and Becca Wasser, *No I in Team: Integrated Deterrence with Allies and Partners* (Washington, D.C.:, Center for a New American Security, December 14, 2022), https://www.cnas.org/publications/reports/no-i-in-team.

Onni Aarne, Tim Fist, and Caleb Withers, *Secure, Governable Chips: Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing* (Washington, D.C.:, Center for a New American Security, January 8, 2024), https://www.cnas.org/publications/reports/secure-governable-chips.

Tim Fist and Erich Grunewald, *Preventing AI Chip Smuggling to China: A Working Paper* (Washington, D.C.: Center for a New American Security, October 24, 2023), https://www.cnas.org/publications/reports/preventing-ai-chip-smuggling-to-china.

[1] Antony J. Blinken, "The Administration's Approach to the People's Republic of China" (speech, The George Washington University, Washington, D.C., May 26, 2022), https://www.state.gov/the-administrations-approach-to-the-peoples-republic-of-china/.
[2] Juan Zarate, *Treasury's War: The Unleashing of a New Era of Financial Warfare* (New York: PublicAffairs, 2013).
[3] U.S. Department of Defense, *National Defense Industrial Strategy* (U.S. Department of Defense, January 11, 2024), https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf; Deputy Secretary of Commerce Don Graves, "Remarks by Deputy Secretary of Commerce Don Graves at the National Foreign Trade Council's Alliance for National Security and Competitiveness" (public event, National Foreign Trade Council, Washington, D.C., January 9, 2024), https://www.commerce.gov/news/speeches/2024/01/remarks-deputy-secretary-commerce-don-graves-national-foreign-trade-councils; *The Treasury 2021 Sanctions Review* (U.S. Department of the Treasury, October 2021), https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf.
[4] Zack Cooper, "Does America Have an Endgame on China?" *ChinaFile*, December 15, 2023, https://www.aei.org/op-eds/does-america-have-an-endgame-on-china/.
[5] Emily Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China* (Washington, D.C.: Center for a New American Security, December 1, 2023), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/EES-No-Winners_Final-1.pdf.
[6] *U.S. National Security Strategy* (Washington, D.C.: White House, October 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.
[7] Secretary of the Treasury Janet Yellen, "Remarks by Secretary of the Treasury Janet L. Yellen on the U.S.-China Economic Relationship" (public event, Johns Hopkins School of Advanced International Studies, Washington, D.C., April 20, 2023), https://home.treasury.gov/news/press-releases/jy1425; Secretary of Commerce Gina Raimondo, "Remarks by U.S. Secretary of Commerce Gina Raimondo on U.S. Competitiveness and the China Challenge" (public event, Massachusetts Institute of Technology, Cambridge, MA, November 30, 2022), https://www.commerce.gov/news/speeches/2022/11/remarks-us-secretary-commerce-gina-raimondo-us-competitiveness-and-china; Jake Sullivan, "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership" (public event, Brookings Institution, Washington, D.C., April 27, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution/; and Blinken, "The Administration's Approach to the People's Republic of China."
[8] Representative Mike Gallagher, "Let's Stop Paying Beijing to Steal Our Gene Code," press release, November 13, 2023, https://gallagher.house.gov/media/in-the-news/lets-stop-paying-beijing-steal-our-gene-code; "A bill to prohibit contracting with certain biotechnology providers, and for other purposes," 118 (S.3558) (2023), https://www.congress.gov/bill/118th-congress/senate-bill/3558?s=1&r=1.
[9] Dan Wang, "Biden Is Beating China on Chips. It May Not Be Enough." *The New York Times*, July 16, 2023, https://www.nytimes.com/2023/07/16/opinion/biden-china-ai-chips-trade.html.
[10] This section draws on analysis and recommendations from Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China*.
[11] Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China*.
[12] For more on "integrated deterrence," see *2022 National Defense Strategy of the United States of America* (U.S. Department of Defense, October 27, 2022), https://media.defense.gov/2022/Oct/27/2003103845/1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPRMDR.PDF.
[13] Stacie Pettyjohn and Becca Wasser, *No I in Team: Integrated Deterrence with Allies and Partners* (Washington, D.C.: Center for a New American Security, December 14, 2022), https://www.cnas.org/publications/reports/no-i-in-team.
[14] Sarah Bauerle Danzman and Emily Kilcrease, "The Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail," *Foreign Affairs*, December 30, 2022, https://www.foreignaffairs.com/united-states/illusion-controls.
[15] Hugo Meijer, *Trading with the Enemy: The Making of US Export Control Policy toward the People's Republic of China* (New York: Oxford University Press, 2016); Tim Hwang and Emily Weinstein, *Decoupling in Strategic Technologies: From Satellites to Artificial Intelligence* (Center for Security and Emerging Technology, July 2022), https://cset.georgetown.edu/publication/decoupling-in-strategic-technologies/.
[16] Emily Weinstein and Kevin Wolf, "COCOM's Daughter?", World ECR, May 13, 2022, https://cset.georgetown.edu/article/cocoms-daughter/; *Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators: Hearing Before the U.S.-China Economic and Security Review Commission* (2022) (statement of Emily Kilcrease, Senior Fellow and Director of the Energy, Economics, and Security Program, CNAS), https://www.cnas.org/publications/congressional-testimony/challenging-chinas-trade-practices.
[17] Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China*; Emily Benson and Catharine Mouradian, *Establishing a New Multilateral Export Control Regime* (Center for Strategic and International Studies, November 2, 2023), https://www.csis.org/analysis/establishing-new-multilateral-export-control-regime.
[18] Emily Kilcrease, Jasper Helder, and Kevin Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council* (January 14, 2022), www.cnas.org/publications/commentary/public-commentskilcreaseus-and-eu-export-control-cooperation-under-the-us-eu-trade-and-technology-council.
[19] The White House, "G7 Leaders' Statement on Economic Resilience and Economic Security," press release, May 20, 2023, https://www.whitehouse.gov/briefing-room/ statements-releases/2023/05/20/g7-leaders-statement-on-economic-resilience-and-economic-security/#:~:text=G7%20Leaders'%20Statement%20on%20 Economic%20Resilience%20and%20Economic%20 Security,-Home&text=Fostering%2.
[20] Kilcrease, *Challenging China's Trade Practices: Promoting Interests of U.S. Workers, Farmers, Producers, and Innovators: Hearing Before the U.S.-China Economic and Security Review Commission*.
[21] Kilcrease, Helder, and Wolf, *Public Comments of Kevin Wolf, Emily Kilcrease, and Jasper Helder Regarding Areas and Priorities for US and EU Export Control Cooperation under the US-EU Trade and Technology Council*.
[22] Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China* (Washington, D.C.: Center for a New American Security, March 2, 2023), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmicand-entity-list-designations-on-china.
[23] In full disclosure, the author is employed by a think tank and the author's spouse is employed by a federally funded research and development center.
[24] For ECRA's statement of policy, see Export Control Reform Act of 2018, 50 U.S.C. § 4811, (2018), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter58&edition=prelim.
[25] *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools: Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*, 118th Cong. 4-5 (2023) (Statement of Kevin Wolf, Non-Resident Senior Fellow at the Center for Security and Emerging Technology), https://www.banking.senate.gov/imo/media/doc/Wolf%20Testimony%202-28-23.pdf.

[26] Wolf, *Advancing National Security and Foreign Policy Through Sanctions, Export Controls, and Other Economic Tools: Hearing Before the Senate Committee on Banking, Housing, and Urban Affairs*.
[27] For ECRA's statement of policy, see Export Control Reform Act of 2018, 50 U.S.C. § 4811, (2018), https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter58&edition=prelim.
[28] *Modernizing Export Controls: Protecting Cutting-Edge Technology and U.S. National Security: Hearing Before the U.S. House of Representatives Committee on Foreign Affairs*, 115th Cong. (2018) (Statement of Kevin Wolf, former Assistant Secretary of Commerce), https://docs.house.gov/meetings/FA/FA00/20180314/107997/HHRG-115-FA00-Wstate-WolfK-20180314.pdf.
[29] White House, "Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy," press release, December 10, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/; Emily Kilcrease, Jason Bartlett, and Mason Wong, *Sanctions by the Numbers: Economic Measures against Russia Following Its 2022 Invasion of Ukraine* (Washington, D.C.: Center for a New American Security, June 16, 2022), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-economic-measures-against-russia-following-its-2021-invasion-of-ukraine.
[30] Theresa Hitches, "'Game On': Raimondo calls for beefing up tech export controls to counter China," Breaking Defense, December 2, 2023, https://breakingdefense.com/2023/12/game-on-raimondo-calls-for-beefing-up-tech-export-controls-to-counter-china/#:~:text=Raimondo%20said%20that%20the%20administration,have%20a%20%24200%20million%20budget.
[31] Alex W. Palmer, "'An Act of War': Inside America's Silicon Blockade against China," *The New York Times*, July 12, 2023, https://www.nytimes.com/2023/07/12/magazine/semiconductor-chips-us-china.html.
[32] U.S. Department of Commerce, *The Department of Commerce Budget in Brief: Fiscal Year 2013* (U.S. Department of Commerce), https://www.osec.doc.gov/bmi/budget/FY13BIB/fy2013bib_final.pdf; "Inflation Calculator," Federal Reserve Bank of Minneapolis, accessed on January 15, 2024, https://www.minneapolisfed.org/about-us/monetary-policy/inflation-calculator.
[33] Bureau of Industry and Security, *Fiscal Year 2023: President's Budget Request* (U.S. Department of Commerce, Bureau of Industry and Security), https://www.commerce.gov/sites/default/files/2022-03/FY2023-BIS-Congressional-Budget-Submission.pdf; Bureau of Industry and Security, *Fiscal Year 2024: President's Budget Request* (U.S. Department of Commerce, Bureau of Industry and Security), https://www.commerce.gov/sites/default/files/2023-03/BIS-FY2024-Congressional-Budget-Submission.pdf.
[34] Bureau of Industry and Security, *Fiscal Year 2024: President's Budget Request*.
[35] "Annual BIS Licensing Archive," Bureau of Industry and Security, accessed on January 15, 2024, https://www.bis.doc.gov/index.php/statistical-reports/licensing-analysis/1906.
[36] Tim Fist and Erich Grunewald, *Preventing AI Chip Smuggling to China: A Working Paper* (Washington, D.C.: Center for a New American Security, October 24, 2023), https://www.cnas.org/publications/reports/preventing-ai-chip-smuggling-to-china.
[37] Gregory C. Allen, Emily Benson, and William Alan Reinsch, *Improved Export Controls Enforcement Needed for U.S. National Security* (Washington, D.C.: Center for Strategic and International Studies, November 30, 2022), https://www.csis.org/analysis/improved-export-controls-enforcement-technology-needed-us-national-security.
[38] The author thanks Tim Fist for the points related to the inefficiency of scaling up existing processes; see also Onni Aarne, Tim Fist, and Caleb Withers, *Secure, Governable Chips: Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing* (Washington, D.C.:, Center for a New American Security, January 8, 2024), https://www.cnas.org/publications/reports/secure-governable-chips.
[39] "Commerce Control List," Bureau of Industry and Security, accessed on January 15, 2024, https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.
[40] National Science and Technology Council, *Critical and Emerging Technologies List Update: A Report by the Fast Track Action Subcommittee on Critical and Emerging* Technologies (National Science and Technology Council and the White House Office of Science and Technology Policy, February 2022), https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.
[41] National Defense Authorization Act for Fiscal Year 2024, 118 H.R. 2670 [1345] (2024), https://www.congress.gov/bill/118th-congress/house-bill/2670/text.
[42] U.S. Department of State, "Military-Civil Fusion and the People's Republic of China," accessed on January 15, 2024, https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.
[43] Jake Sullivan, "Remarks by Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit" (public event, Special Competitive Studies Project, Washington, D.C., September 16, 2022), https://www.whitehouse.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/.

[45] Sullivan, "Remarks by National Security Advisor Jake Sullivan on Renewing American Economic Leadership."
[46] Emily Kilcrease, Tim Fist, Sarah Bauerle Danzman, Ngor Luong, and Emily Weinstein, *Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern* (September 29, 2023), https://www.regulations.gov/comment/TREAS-DO-2023-0009-0049.
[47] See section 734.9 of the Export Administration Regulations at https://www.bis.doc.gov/index.php/documents/regulations-docs/2382-part-734-scope-of-the-export-administration-regulations-1/file.
[48] Bureau of Industry and Security, "Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule)," *Federal Register* Vol. 85, No. 162, August 20, 2020, https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2593-85-fr-51596/file.
[49] Congressional Research Services, *Huawei and U.S. Law* (Congressional Research Service, February 23, 2010), https://crsreports.congress.gov/product/pdf/R/R46693#:~:text=In%20May%202019%2C%20the%20Trump,products%20and%20services%20to%20Huawei.
[50] Sophie Yu and Tony Monroe, "China's Huawei says 2021 revenues down almost 30%, sees challenges ahead," Reuters, December 30, 2021, https://www.reuters.com/technology/chinas-huawei-says-2021-revenues-down-almost-30-sees-challenges-head-2021-12-31/.
[51] Emily Kilcrease, *Noteworthy: The New Russia Export Controls* (Washington, D.C.: Center for a New American Security, March 7, 2022), https://www.cnas.org/press/press-note/noteworthy-the-new-russia-export-controls.
[52] Emily Kilcrease, "How to Win Friends and Choke China's Chip Supply," War on the Rocks, Metamorphic Media, January 6, 2023, https://warontherocks.com/2023/01/ how-to-win-friends-and-choke-chinas-chip-supply/.
[53] "TechInsights Finds SMIC 7nm (N+2) in Huawei Mate 60 Pro," TechInsights, accessed on January 15, 2024, https://www.techinsights.com/blog/techinsights-finds-smic-7nm-n2-huawei-mate-60-pro.
[54] Chris Cook, "Moscow Imports a third of battlefield tech from western companies," *Financial Times*, January 11, 2024, https://www.ft.com/content/96c4f3f8-bd7b-41a3-9e76-7280490a3dbb.

[55] Danzman and Kilcrease, "Illusion of Controls: Unilateral Attempts to Contain China's Technology Ambitions Will Fail."
[56] See 15 CFR § 758.1, "The Electronic Export Information (EEI) filing to the Automated Export System (AES)," https://www.law.cornell.edu/cfr/text/15/758.1.
[57] Analysis and recommendations this section draw from prior testimony provided by the U.S.-China Economic and Security Review Commission, see *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission*, 118th Cong. (2023) (statement of Emily Kilcrease, Senior Fellow and Director, Energy, Economics, and Security Program, CNAS), https://www.uscc.gov/sites/default/files/2023-04/Emily_Kilcrease_Testimony.pdf.
[58] For an overview of the CFIUS interagency process, see the CFIUS website at: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.
[59] See 31 CFR § 800.213 (*covered transaction*).
[60] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[61] See 50 USC § 4565(a)(6) and 31 CFR § 800.215.
[62] See 31 CFR § 800.210 (*covered control transaction*).
[63] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[64] Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins, "Dual use of artificial-intelligence-powered drug discovery," *Nature Machine Intelligence*, 4, March 2022.
[65] Cade Metz and Gregory Schmidt, "Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society,'" *The New York Times*, March 29, 2023, https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html.
[66] See 31 CFR § 800.248 (*TID U.S. business*).
[67] National Science and Technology Council, *Critical and Emerging Technologies List Update: A Report by the Fast Track Action Subcommittee on Critical and Emerging* Technologies.
[68] U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022" (U.S. Department of the Treasury, 2023), https://home.treasury.gov/system/files/206/CFIUS%20-%20Annual%20Report%20to%20Congress%20CY%202022_0.pdf.
[69] U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022" (U.S. Department of the Treasury, 2023), https://home.treasury.gov/system/files/206/CFIUS%20-%20Annual%20Report%20to%20Congress%20CY%202022_0.pdf.
[70] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[71] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[72] U.S. Department of the Treasury, "Committee on Foreign Investment in the United States: Annual Report to Congress, Report Period CY 2022"; Thile Hanemann, Armand Meyer, and Danielle Goh, "Vanishing Act: The Shrinking Footprint of Chinese Companies in the US," Rhodium Group, September 7, 2023, https://rhg.com/research/vanishing-act-the-shrinking-footprint-of-chinese-companies-in-the-us/.
[73] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[74] Kilcrease, *The Role of Investment Security in Addressing China's Pursuit of Defense Technologies: Hearing Before the U.S.-China Economic and Security Review Commission.*
[75] Analysis and recommendations in this section draw heavily on joint work conducted with Sarah Bauerle Danzman, as published in Sarah Bauerle Danzman and Emily Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism* (Washington, D.C.: The Atlantic Council, September 14, 2022), https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sand-in-the-silicon-designing-an-outbound-investment-controls-mechanism.
[76] White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern,* Washington, D.C., August 9, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/08/09/executive-order-on-addressing-united-states-investments-in-certain-national-security-technologies-and-products-in-countries-of-concern/;
[77] Karen Freifeld and Andrea Shalal, "US senators push China investments tracker in defense bill as White House finalizes order," Reuters, July 14, 2023, https://www.reuters.com/world/us/us-senators-push-china-investments-tracker-defense-bill-white-house-finalizes-2023-07-14/.
[78] U.S. House of Representatives Financial Services Committee, "McHenry, Subcommittee Chairs Urge House and Senate Armed Services Committee Leadership to Reject Misguided Outbound Investment Regime, Prioritize Time-Tested Sanctions and Export Controls," press release, November 29, 2023, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409061.
[79] The Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party* (Washington, D.C.: U.S. House of Representatives, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, December 12, 2023), https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/reset-prevent-build-scc-report.pdf.
[80] Danzman and Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism.*
[81] Emily S. Weinstein and Ngor Luong, *U.S. Outbound Investment into Chinese AI Companies* (Center for Security and Emerging Technologies, February 2023), https://cset.georgetown.edu/publication/u-s-outbound-investment-into-chinese-ai-companies/; and Alex Alpers and Eduardo Baptista, "China chip firm powered by US tech and money avoids Biden's crackdown," Reuters, December 13, 2023, https://www.reuters.com/technology/china-chip-firm-powered-by-us-tech-money-avoids-bidens-crackdown-2023-12-13/.
[82] Danzman and Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism.*
[83] Danzman and Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism.*
[84] White House, *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern*; and Karen Freifeld and Andrea Shalal, "US senators push China investments tracker in defense bill as White House finalizes order."
[85] Danzman and Kilcrease, *Sand in the Silicon: Designing an Outbound Investment Controls Mechanism.*
[86] U.S. House of Representatives Financial Services Committee, "McHenry, Subcommittee Chairs Urge House and Senate Armed Services Committee Leadership to Reject Misguided Outbound Investment Regime, Prioritize Time-Tested Sanctions and Export Controls."

[87] Kilcrease, *No Winners in This Game: Assessing the U.S. Playbook for Sanctioning China;* Emily Kilcrease and John Hughes, "It's not time to hit China with financial sanctions – yet," The Hill, January 16, 2024, https://thehill.com/opinion/international/4411407-its-not-time-to-hit-china-with-financial-sanctions-yet/.
[88] Emily Kilcrease, Tim Fist, Sarah Bauerle Danzman, Ngor Luong, and Emily Weinstein, *Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern.*