



Selective Openness

A Framework for Chinese Direct Investment in the United States

BY THE TASK FORCE WORKING GROUP

Peter Cowhey, Chair

Under the auspices of the Task Force on U.S.-China Policy
Co-Chairs: Susan Shirk and Orville Schell

AUGUST 2026

UC San Diego

SCHOOL OF GLOBAL POLICY AND STRATEGY
21st Century China Center

Contents

Acknowledgments 3

About the Task Force Working Group 4

Members of the Working Group..... 5

Executive Summary 6

Main Report 10

Stress Test 1 – Corporate Governance28

Stress Test 2 – Cybersecurity38

Stress Test 3 – Clean Energy46

Stress Test 4 – Life Sciences56

Stress Test 5 – Humanoid Robotics.....66

Acknowledgments

By Susan Shirk

My foremost thanks go to Peter Cowhey, who chaired the Working Group on Chinese Direct Investment in the United States. Peter brought intellectual leadership, policy judgment and sustained commitment to every stage of this undertaking. He guided the group through a complex set of economic, national security and regulatory questions and helped transform its wide-ranging deliberations into a coherent policy framework.

I am also deeply grateful to Orville Schell, my longtime intellectual partner and co-chair of the Task Force on U.S.-China Policy, for his encouragement and collaboration throughout the project.

The members of the Working Group devoted many months to examining the risks, opportunities and policy choices associated with Chinese investment in the United States. In plenary sessions, smaller working groups and numerous exchanges, they tested competing perspectives and shared their expertise with candor and generosity. The quality of this report reflects the seriousness and depth of their engagement.

Special recognition is due to the authors of the five accompanying stress tests on corporate governance, cybersecurity, clean energy, biomedicine and medical devices, and robotics. Their detailed analyses allowed the Working Group to test the report's general framework against the distinct challenges presented by different sectors. These studies added depth, specificity and practical relevance to the Working Group's recommendations.

The project also benefited from the expertise of Henrik Christensen, Wendy Cutler, Elizabeth Economy, Jimmy Goodrich, Ruixue Jia, Shirley Meng, Alex Rogers and Dan Rosen, who offered encouragement and advice at various stages. Their contributions sharpened our analysis, although they bear no responsibility for the report's conclusions or final content.

Lei Guang, executive director of the 21st Century China Center, provided indispensable leadership in organizing and managing the project from its inception through publication. Harris Doshay, Brent Crane, and colleagues at UC San Diego's School of Global Policy and Strategy including Amy Robinson, Virginia Watson and Rosemarie Hanai, contributed editorial, design and production support and helped ensure the report's timely completion.

This undertaking was made possible by the generous support of the Andrew Carnegie Foundation, formerly Carnegie Corporation of New York. I extend particular thanks to Stephen Del Rosso, former vice president of the foundation's International Program, for his steadfast support of the 21st Century China Center and the work of the Task Force on U.S.-China Policy.

About the Task Force Working Group¹

Organized by the UC San Diego 21st Century China Center, the Working Group on Chinese Direct Investment in the U.S. operates under the auspices of the Task Force on U.S.-China Policy, which is co-chaired by Susan Shirk of the UC San Diego 21st Century China Center and Orville Schell of the Asia Society's Center on U.S.-China Relations. The Working Group is chaired by Peter Cowhey, Dean Emeritus of UC San Diego's School of Global Policy and Strategy, and comprises eighteen members drawn from academia, industry, and the policy community, including several former government officials.

Working Group members met virtually seven times from October 2025 to June 2026 to develop and refine the main report. In addition, smaller teams conducted detailed work on three sectoral stress tests and two cross-cutting issue areas: corporate governance, and data and cybersecurity.

The Working Group's report introduces a policy framework of 'selective openness' to govern Chinese direct investment in the United States. This approach protects U.S. national security while simultaneously advancing economic prosperity. We hope the recommendations contained in the report can help inform the work of the newly announced Board of Investment as it seeks to create a government-to-government forum for addressing investment-related issues between the United States and China. More broadly, the report aims to support a predictable and transparent investment environment that makes the U.S. market attractive to overseas investors, including

Chinese investors, while safeguarding critical national interests.

The 21st Century China Center

The mission of the 21st Century China Center is to produce and disseminate impactful evidence-based research about China, and to enhance U.S.-China relations by advancing scholarly collaboration, convening policy discussions, and actively communicating with policy makers and the general public in both countries.

Asia Society Center on U.S.-China Relations

The Center on U.S.-China Relations was founded in 2006 and is based at Asia Society's New York headquarters. The center undertakes projects and events which explore areas of common interest and divergent views between the two countries, focusing on policy, culture, business, media, economics, energy, and the environment.

© 2026 UC San Diego School of Global Policy and Strategy. All rights reserved. 9500 Gilman Drive #0519 La Jolla, CA 92093-0519 china.ucsd.edu

The 21st Century China Center and UC San Diego School of Global Policy and Strategy take no institutional positions on matters of public policy and other issues addressed in the reports and publications they sponsor. All statements of fact and expressions of opinion contained in this report are the sole responsibility of its authors and may not reflect the views of the organization and its board, staff, and supporters.

¹ The views set forth in this report are personal views of the Working Group members and do not necessarily reflect the views of the institutions with which they are affiliated.

Members of the Working Group

1. Charlene Barshefsky ^{**2} — Chair, Parkside Global Advisors
2. Martin Chorzempa — Senior Fellow, Peterson Institute
3. Zack Cooper ^{**} — Senior Fellow, American Enterprise Institute
4. Peter Cowhey — Dean Emeritus and Qualcomm Chair Emeritus, UC San Diego School of Global Policy and Strategy (Chair of the Working Group)
5. Michael Davidson — Associate Professor, UC San Diego
6. Rush Doshi ^{**} — Director, China Strategy Initiative, Council on Foreign Relations and Assistant Professor, Georgetown
7. Thilo Hanemann — Non-resident Fellow, 21st Century China Center, UC San Diego School of Global Policy and Strategy
8. Arthur Kroeber ^{**} — Founding Partner and Head of Research, Gavekal
9. Jonathan McHale — Former Deputy Assistant U.S. Trade Representative
10. Jonas Nahm — Andrew W. Mellon Associate Professor, Johns Hopkins School of Advanced International Studies (SAIS)
11. Gary Rieschel — Founding Managing Partner, Qiming Venture Partners
12. Meg Rithmire — James E. Robison Professor of Business Administration, Harvard Business School
13. Orville Schell ^{**} — Arthur Ross Director of the Center on U.S.-China Relations at Asia Society in New York (Co-chair, Task Force)
14. Schuyler Schouten — Former Senior Associate Counsel to the President and Deputy Legal Advisor to the National Security Council
15. Tim Scott, President and Chief Executive Officer, Biocom
16. Victor Shih ^{**} — Professor and Ho Miu Lam Chair, UC San Diego School of Global Policy and Strategy
17. Susan Shirk ^{**} — Director Emeritus, 21st Century China Center and Research Professor, UC San Diego School of Global Policy and Strategy (Co-chair, Task Force)
18. Paul Triolo — Non-Resident Honorary Senior Fellow on Technology at the Asia Society Policy Institute's Center for China Analysis

2 Two asterisks (**) denote current members of the larger Task Force on U.S.-China Policy who are involved in this project, along with other members of the Working Group.

Executive Summary

The United States needs a more strategic approach to managing Chinese foreign direct investment (FDI) in the U.S. Existing policy is dominated by national security concerns, leading to a framework that evaluates Chinese investment largely through the lens of security risk avoidance. While these concerns are legitimate and often compelling, an exclusively security-first approach also carries long-term economic costs by limiting opportunities to strengthen U.S. industrial capacity, technological competitiveness, and advanced manufacturing.

This report proposes that the United States replace the current de facto presumption against Chinese investment with a framework of Selective Openness—one that neither embraces unrestricted investment nor pursues broad economic decoupling. Instead, it recommends permitting Chinese direct investments that can be appropriately conditioned to demonstrably advance U.S. economic and strategic interests and managing any national security risks through improved governance and oversight of foreign direct investment.

The case for Selective Openness rests on a fundamental shift in the global economy. China has become a world leader in a growing number of industries, including electric vehicles, batteries, robotics, industrial automation, renewable energy, and segments of the life sciences. At the same time, complete economic decoupling is neither realistic nor likely to preserve America's long-term technological leadership. Rather than excluding Chinese capital categorically, the United States should seek to channel it toward investments that reinforce domestic production, create high-quality jobs, strengthen supply chains, expand technological capabilities, and improve

industrial resilience, while protecting American national security.

Achieving this objective requires modernizing the U.S. investment review system. The report recommends expanding the current framework beyond a narrow assessment of national security risks to include a systematic evaluation of the broader economic and strategic benefits that individual investments could provide. It proposes strengthening the Committee on Foreign Investment in the United States (CFIUS) as the central institution for this effort while equipping it with additional tools to evaluate tradeoffs between economic opportunity and security. It shows how the United States government can set conditions to govern investments that advance specific economic objectives much like how the Chinese government has done about American direct investments in China.

To implement a Selective Openness strategy, the report proposes a series of reforms. These include expanding CFIUS jurisdiction to selected joint ventures and greenfield investments; providing clearer Presidential guidance regarding priority sectors; incorporating greater industry and technical expertise into investment reviews to set appropriate economic and security conditions for investments; improving transparency and predictability for investors; and developing standardized policy templates for corporate governance, cybersecurity, and data protection. Rather than relying on rigid prohibitions or static "blacklists," the framework emphasizes flexible, case-by-case assessments supported by enforceable mitigation measures.

The report also recognizes that the global investment landscape has changed. Chinese firms today possess more technological capabilities, greater access to capital, and more investment opportunities outside the United States than at any point in recent decades.

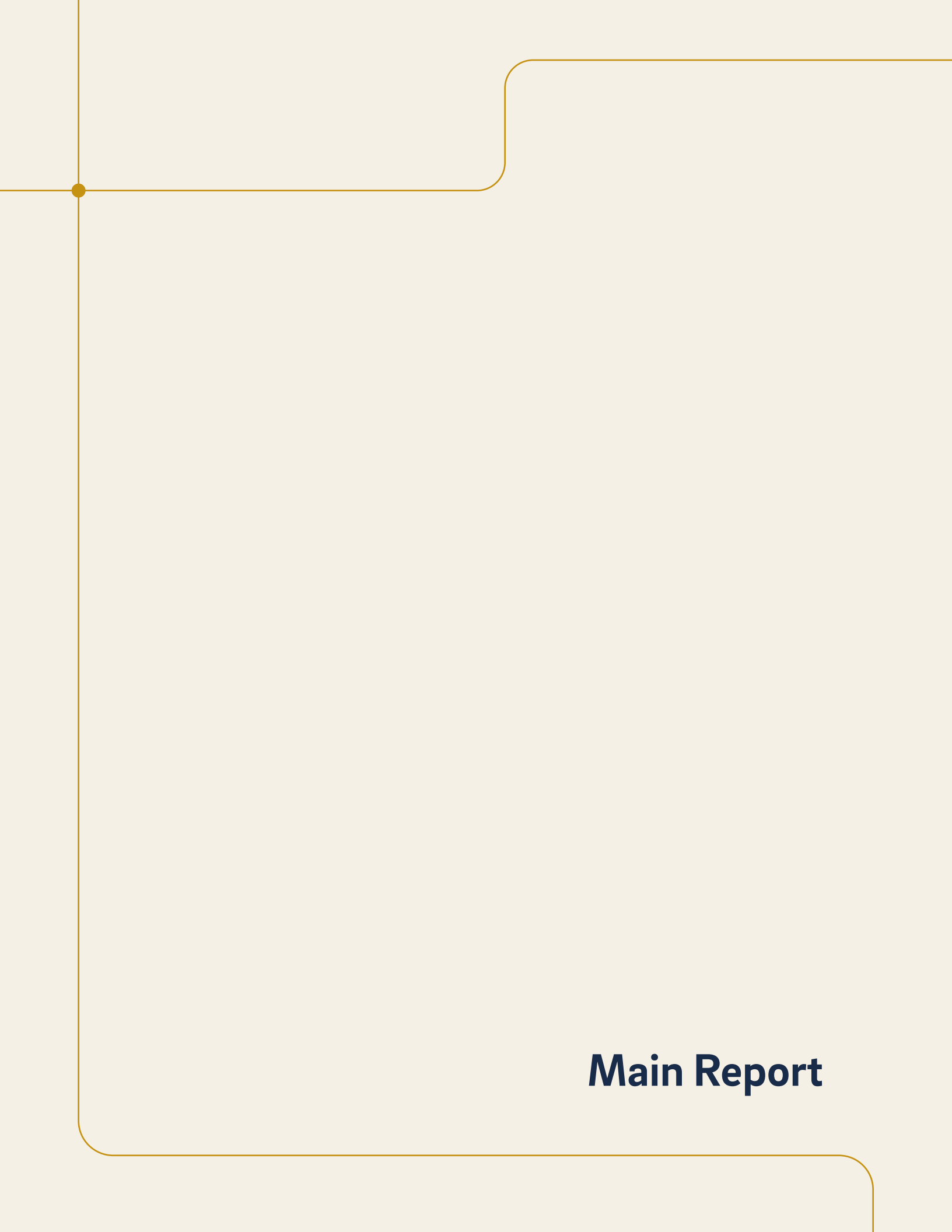
To attract investment that advances its own economic interests, the United States must offer a regulatory framework that is not only rigorous but also coherent, transparent, and predictable. A credible rules-based system would benefit both American stakeholders and responsible foreign investors while preserving the government's ability to block transactions that present unacceptable risks. It also would advance greater coordination with traditional U.S. allies on the terms to govern direct investments from China.

Selective Openness does not require the United States to make a grand bargain with China that trades our traditional security goals for more Chinese investment. Nor does it propose Selective Openness as a substitute for industrial policy, export controls, or other national security tools. Rather, it complements these policies by recognizing that foreign direct investment, when properly structured and governed, can strengthen American competitiveness instead of weakening it. The report stresses that implementing Selective Openness requires a strong governing body with appropriate authorities and analytic resources. The main report is supplemented by two topical and three sector-specific stress tests – covering corporate governance, cybersecurity, clean energy, life sciences, and humanoid robotics – to demonstrate how tailored governance arrangements can simultaneously protect national security and capture substantial economic gains.

In a nutshell, the six policy briefs collectively answer the question of Chinese FDI from six different angles:

1. Why Selective Openness? **(Main Report)**
2. How should governance be structured? **(Corporate Governance)**
3. How should cyber and data risks be managed? **(Cybersecurity)**
4. How can investment build industrial capability? **(Clean Energy)**
5. How should governance vary across different types of biomedical assets? **(Life Sciences)**
6. How should the United States govern emerging embodied AI industries before dependencies become entrenched? **(Humanoid Robotics)**

Ultimately, the choice facing the United States is not between openness and security. It is between a policy that treats every Chinese investment primarily as a threat and one that carefully distinguishes between investments that should be prohibited, those that should be permitted with appropriate safeguards, and those that should be actively encouraged because they advance America's long-term economic strength. A framework of Selective Openness offers a more balanced and strategically sustainable path—one that protects national security while enhancing U.S. industrial competitiveness, innovation, and economic resilience.

The page features a minimalist design with a light beige background. In the top-left corner, there is a decorative element consisting of a small orange dot from which two thin orange lines extend: one horizontally to the right and one vertically downwards. These lines turn at right angles, with the horizontal line ending in a rounded corner and the vertical line continuing down the page. The text 'Main Report' is positioned in the bottom-right area of the page.

Main Report

Main Report

Selective Openness: A Framework for Chinese Direct Investment in the United States

By The Working Group on Chinese Direct Investment in the U.S.³

Foreign direct investment (FDI) has long been one of the most important growth engines of the American economy. By investing abroad, U.S. firms have gained access to global markets, global resources, and global talent pools and made themselves more competitive as a result. Just as importantly, large inflows of investment by foreign companies into the U.S. have brought in new technologies, management practices and knowledge that have made the U.S. economy more competitive and increased opportunities and wages for American workers.

The goal of this Working Group's report is to establish sound principles to govern direct investment from China. Our approach — framed around a strategy of selective openness — would structure Chinese investment on terms that are both consistent with U.S. national security interests and beneficial to the U.S. economy. Our approach to Chinese FDI adopts a long-term perspective; we are not advocating for a grand bargain with Beijing that links economic and security issues. The report may, however, inform the work of the newly announced Board of Investment aimed at providing a government-to-government

forum for discussing investment-related issues. It can also help create an environment attractive to overseas investors.

Selective Openness: An Overview of Our Approach

Over the past decade, national security concerns have been the most important reason that the U.S. government has discouraged Chinese investment in the U.S. Meanwhile, Chinese firms have come to lead sectors where the U.S. lags, including electric vehicles, batteries, solar energy, robotics, high-speed rail and industrial automation. One option for addressing these gaps in American capabilities would be to allow direct investment from China, just as U.S.-Japan trade imbalances in the 1980s and 1990s were partly resolved through Japanese automotive-sector investments in the U.S.

There is considerable skepticism in Washington policy circles about continued economic and technological interdependence with China. We do not attempt to resolve this broad strategic debate. Instead, we address a narrower question: Could direct investment from China in the American economy develop in a productive, secure manner? This report outlines how it could be done. We propose that the U.S. should adopt a selective openness framework grounded in practical risk management to attract Chinese investment in a manner that will fortify, not undermine, U.S. industrial capacity and national security.

National security concerns also existed in the case

³ The Working Group on Chinese Investment in the U.S. is chaired by Peter Cowhey and convened by the Task Force on U.S.-China Policy, a consortium of leading China specialists convened by Asia Society's Center on U.S.-China Relations and the 21st Century China Center at UC San Diego's School of Global Policy and Strategy. Supported by the Carnegie Corporation of New York and co-chaired by Orville Schell and Susan Shirk, the Task Force has operated continuously since 2015. The views expressed in this report are those of the Working Group members and do not necessarily reflect the views of their affiliated institutions.

of Japan, albeit less prominently given Japan's status as a U.S. treaty ally and the clearer delineation between military- and civilian-use products prior to widespread digitization. Welcoming Chinese investment today sparks greater political anxieties and legitimate policy concerns for three main reasons:⁴

- The overall U.S.-China security relationship is one of profound distrust if not outright hostility.
- Under Xi Jinping (since 2012), the lines between businesses and the Chinese state have blurred because of the leadership's efforts to strengthen military capabilities through civil-military fusion, the sprawling reach of state funding in frontier sectors, and the broad sweep of laws that grant the state legal grounds to interfere in firms.⁵
- The U.S. and China are both high-tech economies — sectors and products that are seen as "critical and emerging technologies" or relevant for "critical infrastructure" cover a broad range and are poised to expand.

Chinese investment and ownership in key sectors within the U.S. raise serious security and economic concerns about data collection, transmission and storage; the potential weaponization of consumer and industrial products; supply chain chokepoints that create strategic vulnerabilities; intellectual property theft; and the erosion of the U.S. defense industrial base.

This report proposes a roadmap to address these challenges by clarifying the strategic and economic tradeoffs involved in Chinese FDI in the U.S. It recommends adjustments to the review authority and decision-making process overseeing direct investment from China. While other authorities play a role in this governance task, and must be appropriately coordinated with our strategy, we focus especially on the Committee on Foreign Investment in the United States (CFIUS), the U.S. government body that reviews foreign investments for potential national security risks. CFIUS is the logical anchor for coordinating complementary policy instruments. We support expanding CFIUS's jurisdiction to cover more clearly the formation of certain new joint ventures involving Chinese investments, as well as greenfield investments (in which a parent company creates a new subsidiary from the ground up). We also recommend new tools — referred to here as "templates" — to better enhance economic returns and expand the policy instruments available for risk management.⁶

Many proposals for Chinese investment either pose unacceptable security problems or offer insufficient economic benefits. In contrast, our selective openness framework seeks to use Chinese investment to advance U.S. economic objectives while establishing additional policy safeguards to mitigate risk. Central to our approach

4 The proposed acquisition of Fairchild Semiconductor was nonetheless the impetus for the creation of the Committee on Foreign Investment in the United States (CFIUS). Executive Order 11858 (May 7, 1975) directed CFIUS to "monitor the impact of foreign investment in the United States" and review investments that "might have major implications for United States national interests." When Congress later established a statutory framework for CFIUS, it considered authorizing reviews based on both national security and "essential commerce" considerations, but ultimately limited CFIUS jurisdiction to national security.

5 See Margaret M. Pearson, Meg Rithmire and Kellee S. Tsai, "China's Party-State Capitalism and International Backlash: From Interdependence to Insecurity," *International security* 47, no. 2 (2022): 135-176, https://doi.org/10.1162/isec_a_00447.

6 The current authority of CFIUS includes certain real estate transactions and a limited subset of greenfield investments. Any expansion of CFIUS jurisdiction would require careful tailoring to avoid effectively creating a review process for investments from all countries.

is recalibrating the U.S. government oversight process. To that end, we recommend aligning individual transaction reviews with broader diplomatic, national security and economic policy goals.

Choices for American Economic Policy

Our recommendation to expand the focus of the investment screening process for Chinese direct investments in the U.S. reflects our conviction that security alone should not determine an investment's desirability. Our emphasis on the additional dimension of strategic economic benefits rests on our understanding of the consequences of continuing our current economic path or pursuing major alternatives. These choices rest on two basic questions.

1. Capital from China continues to flow to the U.S. What is the desired mix of capital flow?

Absent a fundamental reset of the bilateral economic relationship, the United States cannot simply reject Chinese capital. As long as the U.S. runs a significant current account deficit with China, it will, by definition, continue to absorb net capital inflows from China. The question thus becomes: what types of capital inflows should U.S. policy favor?

Historically, these flows have largely involved China's central bank purchasing "safe haven" assets like U.S. Treasury securities. In the 2010s, Beijing started allowing firms to deploy surplus foreign exchange into outbound FDI on a greater scale, leading to a surge in Chinese outbound investment to the U.S. between 2014 and 2017. As Beijing subsequently tightened capital controls and U.S. scrutiny on Chinese FDI

increased, Chinese capital flows shifted back to more "passive" forms. These included continued Treasury purchases by the central bank (often routed through third markets like Luxembourg or Belgium) as well as portfolio investment in U.S. equities and debt by state banks, sovereign investment vehicles and, to a lesser extent, approved private asset managers. Over the past decade, Beijing has also increasingly relied on state-owned banks to recycle foreign exchange surpluses through cross-border lending. This has included financing for infrastructure projects and credit facilities for multinational corporations, especially in lower-income economies. To the extent that beneficial investment in the United States draws capital away from China's market-distorting investment in other countries — investment that often undermines the U.S. competitive position in those markets — the benefits can be twofold: strengthening U.S. exports while building domestic capacity.

Going forward, America's trade deficit with China is likely to persist. Policymakers should articulate a vision for their desired composition of capital flows from China. Should policymakers favor more passive holdings of U.S. debt and equity securities and lending to U.S. companies? Or should the U.S. encourage more active investment through direct investment in the U.S. real economy?⁷ Both approaches are viable but carry different economic implications. Passive flows tend to encourage higher asset prices and lower marginal financing costs for the U.S. government and companies. By contrast, FDI is more likely to generate more tangible economic benefits, such as jobs, technological innovation, tax revenue and broader spillover benefits.⁸

7 U.S. tariff policy also shapes the landscape for Chinese foreign direct investment. This report focuses on the underlying logic of investment decisions and their economic consequences rather than their interaction with tariff policy.

8 Pearson, Rithmire and Tsai, "China's Party-State Capitalism."

2. What are the alternatives to full decoupling from China?

We reject a full economic decoupling from China as a practical strategy. Constructing a China-free economic zone that is both insulated from Chinese competition and globally competitive is unlikely to be economically sustainable, even with cooperation from U.S. allies.

China has evolved into a formidable technological power. Of course, Chinese firms have long benefited from expansive government support, including a protected home market, substantial subsidies and large-scale infrastructure investment. But many Chinese firms can now compete globally even if government support declined substantially. China is also now the world's largest manufacturing economy, with output roughly equal to that of the U.S., Japan, Germany and South Korea combined and is a major driver of innovation across a range of technologies. Despite ongoing protectionist measures by the U.S. and other countries, a growing number of Chinese industries are likely to become even more globally competitive in the coming decades. For U.S. firms to preserve existing advantages over Chinese competitors — or to close gaps where U.S. firms lag — three realistic pathways exist:⁹

Comparative advantages plus expanded U.S. industrial policy

The United States could continue emphasizing its strengths in services, research and development, design and high-value innovation while ceding to China many advanced manufacturing sectors where

Beijing already holds significant structural advantages. This approach would likely accelerate the erosion of America's industrial base. Although stronger industrial policy could partially offset losses, China's lead across numerous strategic growth sectors raises serious doubts about whether the U.S. can mobilize sufficient resources, coordination and long-term policy discipline to close all major gaps.

Expanded U.S. investment in China

American companies could deepen investments in China to benefit directly from its increasingly sophisticated innovation ecosystem, advanced production capabilities and evolving technology developments. Many multinational firms, including German carmakers and global industrial automation leaders, are already pursuing this model. This path's desirability is offset by the fact that it strengthens U.S. firms' global competitiveness without substantially enhancing domestic American production systems, human capital or industrial resilience. Moreover, national security restrictions increasingly limit U.S. investment in sectors tied to Chinese defense, intelligence or civil-military fusion.

More Chinese direct investment in the U.S. under selective openness

A third path would encourage carefully structured Chinese direct investment in the U.S. — particularly in advanced manufacturing — to strengthen American industrial competitiveness, economic security, workforce capabilities and technological learning. This approach would capture many of the benefits for the U.S. that were historically associated with

⁹ Enhancing the long-term competitiveness of U.S. firms depends on a broader set of domestic policy reforms, not solely foreign investment policy. For example, China has largely closed the gap with — and is projected soon to surpass — the United States in expenditures on basic and advanced applied research, reflecting differences in government funding priorities. This report focuses more narrowly on managing future Chinese investment.

American firms investing in China, including access to process know-how, technological capabilities and competitive pressure. Selective openness does assume that all manufacturing investments will serve American interests. It scrutinizes risks such as deepening dependence on Chinese supply chains or deindustrialization. Properly managed – and paired with complementary economic policies, this strategy could adapt the formula China used for decades to absorb foreign technology and industrial know-how, helping revitalize U.S. production ecosystems and encourage American firms to expand at home.

All things being equal, rising Chinese global competitiveness would naturally generate a significant increase in Chinese direct investment into the U.S., much as German and Japanese investment expanded in the U.S. in the 1980s. All things, however, are not equal. The challenge is that China is not merely an economic competitor – China is a geopolitical rival at a scale that presents major security concerns.

The goal of U.S. policy, therefore, should be to create an inbound investment regime that generates maximum economic and technological gain while minimizing risk; strengthens U.S. industrial and human capital development; preserves national security; and uses investment policy as a tool of strategic economic statecraft

China itself successfully leveraged foreign capital under similarly selective principles for decades. The U.S. can pursue a comparable model – one designed not to protect specific incumbent firms, but to strengthen the national ecosystem of innovation, efficient production and human capital development.

As appendices to the report, we offer three industry-specific “stress tests” of our framework. We focus on green technology, robotics and the life sciences. All

three are areas of established or emerging Chinese strength in which direct Chinese investment could benefit the U.S. economy substantially if security concerns are properly managed. Proposed investment models range from licensing technology to forming joint ventures or foreign-owned subsidiaries. Each comes with tailored requirements for corporate governance, cybersecurity and, if necessary, structural separation of software, hardware and data storage.

Our selective openness framework is not an open-ended invitation to Chinese investment on terms set by private firms. It is a pragmatic approach to balancing two imperatives: protecting U.S. national security while enhancing the economic benefits of engagement. Cybersecurity threats are ubiquitous in this digital era, especially in fields such as critical infrastructure. It is appropriate to require rigorous reviews of any Chinese involvement in digital systems for critical infrastructure and defense. These may well lead to banning certain types of investments altogether.

At the same time, a purely risk-first approach – one that rejects Chinese investment unless it presents no conceivable risk – creates strategic dangers of its own. Although such an approach may reduce immediate security concerns, it could increase longer-term strategic vulnerabilities by isolating the U.S. from one of the world’s most important centers of technological innovation, industrial capability and competitive pressure. Over time, that isolation would weaken U.S. technological dynamism, reduce industrial competitiveness and erode broader economic security.

For this reason, establishing an appropriate governance framework for selective openness is critical. Because of the growing options for Chinese investors, investment choices are a two-way process.

U.S. policy must be credible, strategically coherent and economically attractive if it is to shape the future direction of Chinese capital, as we discuss next.

The Perspective of Chinese Investors

The U.S. is an important market for Chinese investors, but many other attractive alternatives exist. Future Chinese direct investment in the U.S. will depend on the credibility and predictability of the U.S. investment environment. Therefore, a policy of selective openness must consider the need for credibility.

Chinese direct investment flows into the U.S. have plunged dramatically since 2016, even as China has maintained substantial (albeit reduced) flows into the rest of the world. The decline in Chinese investment in the U.S. reflects, in part, rising geopolitical tensions. U.S. restrictions on Chinese participation in strategically important supply chains — including information and communications technology and services (ICTS) rules that have effectively excluded Chinese EVs from the U.S. market — and expanded CFIUS authorities following 2018 legislative reforms have significantly increased barriers to Chinese investment.

However, the larger structural story lies in three major changes in the global opportunity landscape facing Chinese investors. This structural story must be properly understood for the U.S. to fully take advantage of Chinese FDI.

First, Chinese companies are internationalizing earlier. Intense domestic competition, chronic production overcapacity and aggressive price wars are pushing Chinese firms to seek overseas markets much earlier in their development cycle. Developing countries are especially attractive because they typically feature less saturated competitive environments than China's

domestic market and have fewer foreign competitors matching Chinese firms on price-to-performance ratios. Developing countries also have significant infrastructure needs that align with China's strengths in large-scale industrial and construction projects.

Second, China's domestic capital ecosystem has matured. China's aggressive push for indigenous technology development has expanded domestic funding options. Chinese venture and industrial capital now display greater tolerance for technological risk, with local and central government-backed RMB funds increasingly dominating investment pools. In some sectors, such government-linked lenders now account for roughly 80% of available funding.

Third, the perceived technological necessity of investing in the U.S. has diminished as China narrows or closes technological gaps in key sectors. Chinese investors increasingly view access to the U.S. market as less essential for obtaining the best technology. Simultaneously, venture capital returns within China can outperform U.S. opportunities. China's domestic and Hong Kong capital markets have become more predictable, and Chinese firms now possess broader global options for both growth and technological upgrading.

Taken together, these shifts mean that the U.S. is no longer the singular compelling destination it once was for Chinese capital. Chinese investors continue to see attractive opportunities in the U.S., which remains the largest and most dynamic consumer market in the world. Importantly, however, they are likely to be less tolerant of regulatory unpredictability. In addition to CFIUS scrutiny, Chinese investors must now navigate a growing array of overlapping political and regulatory risk from other federal, state or local agencies. This fragmented environment creates uncertainty even for transactions that may survive CFIUS review,

leaving investors uncertain about when — or whether — they have truly satisfied U.S. regulatory expectations. We believe a more transparent and systematic review of these investments through our selective openness framework could slowly establish greater confidence among U.S. and Chinese stakeholders.

In short, the United States remains an important market for Chinese companies and investors, but it is no longer an indispensable one. For selective openness to work, the U.S. must offer a more coherent, credible and predictable investment environment. Both sides need greater clarity about the terms of permissible or desirable investment.

On the Chinese side, the emerging export control regime has hardened significantly over the last year. In June 2026, China's State Council published the Regulations on Outbound Investment, effective July 1, 2026, which established a more comprehensive approach to Chinese direct investment that links investment to export control, national security review and anti-foreign sanctions. Chinese government controls will also require clarification and negotiated easing so U.S. investment partners can be confident they will retain access to technologies needed for viable long-term investment. Both sides would benefit from a clearer and more institutionalized framework governing investment. While each government will continue to prioritize core national security objectives, there is now an opportunity for China to moderate or pause the expansion of technology export controls in selected sectors and for the U.S. to adopt a pragmatic yet clearly defined approach.¹⁰

Strengthening the CFIUS Strategic Framework

Below, we present key points outlining both the current state of U.S. investment review and beneficial changes to the system.

Current U.S. investment regulation prioritizes national security risks over broader national economic security objectives.

On the security side, CFIUS has proven to be a flexible and adaptable institution, with broad jurisdiction to review, mitigate or block FDI in the U.S. For example, fears about potential loopholes in Chinese venture capital investment in U.S. startups have been addressed by extending CFIUS jurisdiction to a wide range of nonpassive investments, including those that confer broad rights or access to material nonpublic technical information in sensitive firms. However, CFIUS was not designed to systematically weigh the economic benefits of transactions against their security risks. Given that both governments have now articulated ambitious targets for bilateral investment, an expanded and more balanced review framework is warranted.

The security-first orientation of CFIUS and broader U.S. policy toward Chinese FDI is fundamentally reactive, often at the expense of a more proactive economic strategy.

¹⁰ Morrison and Foerster, "China's ODI Rules Just Changed — Here's What It Means for Cross-Border Tech Transactions," June 4, 2026, <https://www.mofo.com/resources/insights/260604-china-s-odi-rules-just-changed>.

Absent presidential direction or statutory reform, CFIUS lacks a formal mechanism to identify or encourage specific investments, or categories of investment, that could advance U.S. national economic interests. As a result, the policy evolution of CFIUS has tended to underemphasize the strategic value of selectively permitting foreign investment where it could remedy weaknesses in American economic capabilities.

Two developments exemplify this dynamic. First, by statute, CFIUS must certify that transactions pose no unresolved national security concerns, a highly risk-averse standard that tends to favor passive minority investments over more strategic investment involving deeper transfers of resources and expertise. Second, recent administrations have restricted or heavily scrutinized investments even from allied or partner country firms due to stated concerns with the investor's ties to China or Chinese investments. This has reinforced a precautionary posture toward FDI.¹¹

In contrast to the American approach, many other countries also consider economic “net benefits” from FDI by doing a cost-benefit analysis of risks and rewards.

While formulas vary, terms can often be set in ways that contribute significantly to building national economic and technological capabilities while managing security risks. CFIUS legislation recognizes that such screenings can be effective in risk management. Though CFIUS is authorized to coordinate with other countries on investment security screening for a presumption of approval of their firms' direct investments in the U.S., it has not developed regular mechanisms for doing so.

A consistent framework of review, mitigation and verification would better align Chinese investments with U.S. economic priorities while addressing security risks through a more systematic policy architecture.

At present, the U.S. government's assessments of Chinese investment proposals remain largely ad hoc, opaque and heavily transaction-specific. This creates uncertainty not only for American stakeholders but also for prospective Chinese investors, who often lack clear positive benchmarks for structuring investments that align with published U.S. policy objectives. A more coherent framework could bolster both U.S. public and Chinese investor confidence by providing clearer guidance on how investments can meet American economic needs while satisfying national security requirements.

Several policy options could strengthen a more integrated system:

Issue presidential-level strategic guidance to CFIUS and the private sector.

The executive branch could issue formal guidance identifying categories of investments, sectors or safeguards that would be more likely to qualify for streamlined review or a more favorable review standard.

¹¹ The Foreign Investment Risk Review Modernization Act of 2018, among other authorities, provides much of the current statutory authority governing CFIUS reviews.

It would also provide guidance to other federal authorities that they should work with the revised CFIUS process on coordinating their policies with the presidential guidance. Such guidance would preserve case-by-case security review authority while creating clearer expectations for investors. It could also identify sectors in which foreign investment may be particularly valuable to U.S. economic resilience and instruct CFIUS on whether and how to weigh broader economic benefits alongside security concerns.

Consult industry and independent experts more systematically in a sector- or technology-focused process, separate from individual confidential transaction reviews, to improve U.S. government's assessments.

While the U.S. government is good at risk assessments, this is a complex task. Sometimes, the government misses a risk or unduly exaggerates risk scenarios. Outside advice beyond ad hoc lobbying can sharpen analyses. Such consultation should also address the merits of supply chain restrictions on Chinese inputs that may unnecessarily foreclose economically beneficial investment.

Embrace greater transparency and public communication.

While certain national security considerations require confidentiality, the current system often provides insufficient explanation for decisions, contributing to investor uncertainty and public skepticism. More transparent public rationales — similar to how federal courts handle national security issues in cases or CFIUS “due process letters” — could improve credibility, clarify precedent and help justify investment decisions favorable to broader national interests without compromising confidentiality.

Creating Innovative Policy Templates

Selective openness would benefit from a more robust set of criteria and policy tools for assessing risks, advancing strategic economic objectives and crafting effective mitigation strategies. We propose four complementary policy templates.

The first three are: (1) a systematic approach to the corporate governance of Chinese investments in the U.S.; (2) measures for addressing cybersecurity and data management challenges in a digitally enabled economy; and (3) a framework for assessing the potential benefits and risks associated with different forms of Chinese direct investment.

The fourth template draws on the growing use of stress tests in regulatory and governance settings. Stress tests can complement formal policy guidance by helping policymakers identify vulnerabilities, refine assessment frameworks, and improve policy design through practical, case-based analysis.

1) We can require using specialized corporate governance mechanisms for Chinese investment to bolster risk management while preserving economic gains and safeguarding American security interests.

When regulating complex and dynamic market environments, regulators often avoid detailed micro-regulation in favor of broad design principles for risk mitigation. Such principles allow firms flexibility in implementation while ensuring government oversight in monitoring, testing and review. Properly crafted, principles prohibit certain behaviors and require risk mitigation for other behaviors and market structures.

A forthright embrace of specialized corporate governance mechanisms can support more innovative and effective national security mitigation agreements while protecting U.S. interests. Some investments will pose unacceptable risks outright — others will offer benefits too marginal to justify those risks. But where U.S. benefits are substantial and risks are manageable, we recommend customizable mitigation templates built around five core principles — explored further in our sectoral stress tests and in the appendices on cross-cutting issues such as corporate governance and management of cyber risk options. As the sectoral stress tests illustrate, the governance principles apply differently based on which of the three principal models for foreign investment, i.e. licensing, joint ventures, or wholly-owned foreign subsidiaries as described below, are involved. The core principles are:

- *Transparency:* Corporate structures and practices should allow U.S. authorities, partners and potentially the public to understand investor identity and ownership, networks and relevant business practices.
- *Continuous monitoring:* Mechanisms should allow iterative review of corporate practices and entities to ensure long-term national security compliance despite changing market conditions.
- *Supplier diversity:* Investors should avoid single points of failure by diversifying suppliers, service providers and broader ecosystem participation.

Investors can be required to adopt practices to assure expected investments in research and development, a diversity of vendors and market space for healthy competition.

- *Structural separation:* Sensitive activities, such as data collection, storage or actions connecting to critical infrastructure, should be insulated from parent companies where necessary. Separation ensures direct involvement by a U.S. entity in sensitive activities but also ensures that U.S. providers and the broader U.S. corporate ecosystem benefit from increased foreign investment.
- *Enforcement provisions:* Clear penalties, including divestiture, should be built into agreements to ensure credible enforcement while maintaining reasonable investor protections. Regulatory precedents provide a basis for designing such provisions.

2) The U.S. should establish a template for cyber risk mitigation (including cyber and data security) for possible investments by foreign entities of concern.

As digital processing and data increasingly underpin nearly all sectors of world commerce, vulnerabilities, including software sabotage and the misuse of valuable data, are becoming ubiquitous. More consistent mitigation frameworks, adjusted to specific cases, would improve regulatory predictability while preserving national security flexibility. Compliance with the template would not preclude rejection based on specific security concerns. However, important precedents demonstrate how risk mitigation could work. Our appendix on cyber risk analyzes Tesla's

operations in China and TikTok's U.S. spinoff. Details vary by case, but the fundamentals are similar enough to craft templates as starting points.

Effective cybersecurity in business requires deep integration into the fundamentals of corporate governance and management practices. Given such, we organize the starting principles for cybersecurity risk management in terms of corporate governance principles.

- *Structural separation:* Separate corporate entities with specialized governance for highly sensitive digital functions, especially control of algorithms. TikTok had to create a separate U.S. entity with 80% American ownership. ByteDance also licensed its code perpetually to Oracle, which would then retrain and modify algorithms to meet security concerns.
- *Vendor diversification:* Modern digital architecture embraces the principle of modularity, a design that allows individual components (software or hardware) to be swapped out in a system. While not costless, it is usually affordable and technically feasible. China required Tesla to swap out its mapping system and install one from Baidu. The U.S. Commerce Department is requiring modular swaps of subsystems for security reasons in new U.S. cars.
- *Transparency, continuous monitoring and enforcement:* Both Tesla in China and TikTok in the U.S. have reporting obligations on how they comply with requirements for local data storage (and restrictions on cross-border data flows).

3) Assessment templates could provide clearer market guidance on how the U.S. government will evaluate the net benefits of investment based on the channel for direct investment.

Expected net benefits depend on the form of the investment. Clearer guidance on how investment structure shapes U.S. risk analysis can build confidence among both American stakeholders and Chinese investors.

This report lays out three possible channels through which the U.S. economy might attract Chinese capital or technology. These serve as starting points for templates that could guide both investment design and government scrutiny while still allowing for case-specific adjustments, including rejection where necessary.

These three investment channels are: licensing, joint ventures and foreign-owned subsidiaries. Each model presents distinct tradeoffs with respect to economic gains, technology transfer and national security. Our stress tests illustrate further dimensions of the tradeoffs within three ownership structures.¹²

¹² Licensing refers to contractual arrangements under which one firm grants another the right to use its technology or know-how in exchange for royalty or licensing payments over a specified period. Joint ventures are investments in which two or more parties hold significant ownership stakes and jointly manage the enterprise. Foreign-owned subsidiaries are operations in which a foreign investor holds a controlling ownership interest and provides the subsidiary's technology, management, personnel and business strategy, subject to applicable commitments regarding localization, technology transfer and related requirements. Such subsidiaries may be established as greenfield investments or through the acquisition of an existing U.S. firm.

Licensing Agreements

Advantages

- Lowest political risk
- U.S. firm retains operational control
- Rapid technology acquisition without equity entanglement
- Known upfront costs
- Easier exit if geopolitical tensions escalate
- Clear contractual boundaries

Limitations

- Ongoing royalty payments create revenue leakage
- Limited tacit knowledge transfer — firms acquire codified technology (the “recipe”) but not manufacturing expertise (the “cooking skills”)
- Risk of technology obsolescence as licensor advances
- Potential contractual lock-in for upgrades and process improvements
- Minimal integration into partner’s innovation networks

Joint Ventures

Advantages

- Shared investment risk
- Deeper knowledge transfer through colocation of personnel
- Potential for co-innovation and joint IP development
- Access to partner’s supply networks
- Governance structures can include technology transfer milestones

Limitations

- Governance complexity and potential for deadlock
- Risk of U.S. partner becoming “assembler” while Chinese partner controls core competencies
- IP leakage concerns
- Difficult and costly exit
- Potential conflicts over reinvestment priorities versus dividend distribution
- Risk of asymmetric learning if Chinese partner dominates technical functions

Foreign-owned subsidiaries

Advantages

- Potential for knowledge spillovers to local workforce

- No governance conflicts or coordination costs
- Rapid scaling without partner negotiation
- Full technology integration
- Workforce gains exposure to world-class manufacturing techniques
- Foreign firms can bring their own subsidiaries, but their presence also creates demand for local supplier networks and learning opportunities

Limitations

- Knowledge spillovers confined to individual workers, not U.S. firms
- Limited technology transfer to domestic companies absent a robust local supply ecosystem
- Profits repatriated to parent company
- U.S. firms do not necessarily build institutional capabilities if foreign firm does not rely on a local supplier network
- Requires preexisting capacity in regional economy to absorb the subsidiaries

4) Selective “stress tests” should be conducted jointly between U.S. government agencies and outside experts drawn from industry and research centers.

Stress tests can help determine where current U.S. approaches may be either overly restrictive or insufficiently cautious across sectors such as life sciences, energy, automobiles and robotics. Accordingly, sector-specific case studies should be used to refine the assessment models proposed in this framework. For example, some experts in the biomedicine/device field argue that current risk assessments are overly cautious with respect to drug development partnerships while insufficiently attentive to the risks associated with Chinese control of certain U.S. production assets. This report’s stress tests illustrate how such evaluations can be conducted using the investment, corporate governance and cybersecurity risk frameworks developed here.

Implementing the Framework for Selective Openness

- A selective openness framework requires a better organized and more fully staffed U.S. government system than currently exists. The proposed U.S.-China Board of Investment would be unlikely to achieve its desired goals for the American economy while maintaining security safeguards without a revamped national security decision process for investments from China. Fortunately, CFIUS provides a strong foundation and, as a committee chaired by the U.S. Treasury Department, it is at the nexus of national security and economic policy. However, advancing economic security through Chinese investments will require broader economic and security analysis, expert consultation, customized economic commitments and more systematic monitoring that goes beyond the traditional focus of CFIUS.
- The U.S. should avoid rigid “black” or “white” lists for Chinese investment, as such lists can become outdated and overly rigid. Instead, template-based case-by-case analysis offers greater adaptability to changing technological and geopolitical realities.

- The Chinese and U.S. governments could test the framework of selective openness in practice by building on the stress tests proposed in this report. For example, policymakers could designate one or two industry segments as pilot sectors for expedited consideration of potential Chinese investments under the goals and principles of a selective openness framework. Practical experience in structuring investment conditions and monitoring their implementation can help build confidence in the viability and effectiveness of the framework.
- Other OECD economies are developing their own versions of "selective investment" frameworks. The U.S. should make fuller use of existing authorities under CFIUS laws and regulations to promote cooperation across these systems, helping align screening frameworks in ways that allow allied investors and U.S. investors operating in their markets to navigate security reviews more efficiently and predictably.
- This framework will not address all U.S. economic challenges highlighted in our stress tests. Complementary policy tools such as tariffs, research and development investment and workforce training programs for advanced manufacturing remain essential. The stress tests illustrate how such market access and industrial policy instruments can help "steer" the level of Chinese FDI across industries. Ultimately, the type of direct investment (for example, a joint venture) welcomed from China may depend on the economic policy goal relevant to that enterprise.

Additional Comments by Working Group Members

Zack Cooper:

In recent months, Beijing has floated the promise of substantial Chinese investments in the United States, likely in exchange for concessions from Washington on security issues, including Taiwan. In my view, agreeing to a grand bargain of this sort would be a massive mistake. American policymakers should not bet on Chinese promises of investment in the United States materializing, nor should they make concessions on security issues in exchange. If, however, U.S. leaders were to consider accepting Chinese foreign direct investment outside this construct, then I believe this report sets forth a rigorous framework to safeguard U.S. security interests while maximizing the potential benefits to the U.S. economy. It should be noted that for such an effort to ultimately prove beneficial to the United States, it would require broad support from across the American political spectrum as well as stringent verification and consistent enforcement by U.S. officials - features that have been infrequent in Washington's recent approach to its economic relationship with China.

Rush Doshi:

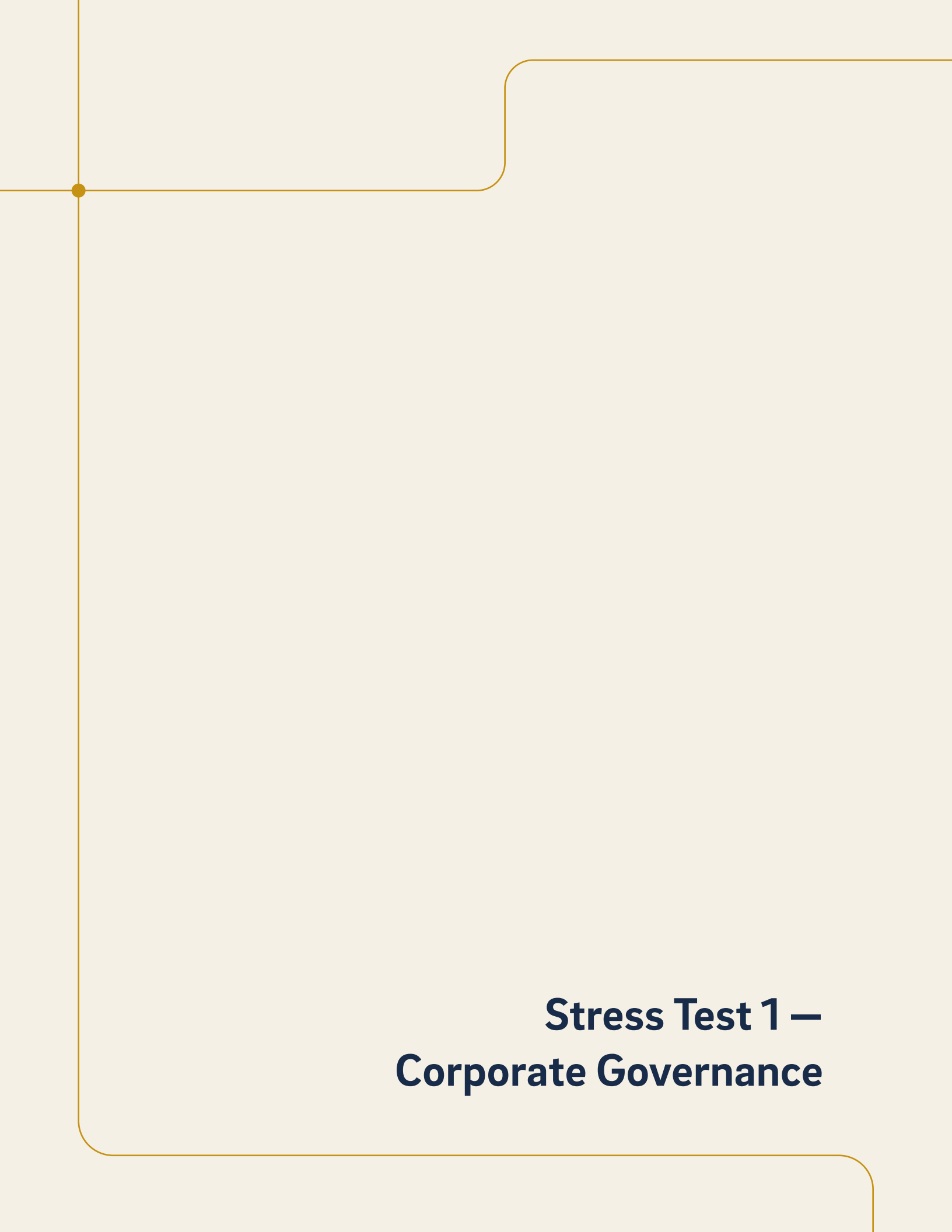
I am grateful to have been a part of this study group and endorse the group's conclusion that Chinese investment can, under some conditions, increase U.S. industrial and technological capability. The key question lies in specifying these conditions, and I would make two points of emphasis regarding them, drawing from the report's stress tests. These should be at the very forefront of policymaker thinking.

First, not all manufacturing investment is equal: some investments, even where no national security threat is found, would accelerate deindustrialization and supply chain dependence rather than spur reindustrialization, and should be prohibited. Investments should be allowed only when they strengthen U.S. suppliers, localize high-value production in the United States, source critical inputs from non-China sources to avoid dependencies, and transfer meaningful skills and process knowledge. They should not confine Americans to final assembly or embed continued dependence on Chinese inputs, equipment, technology, or services. For example, as the stress tests discuss, Chinese investment in auto assembly plants in the United States that rely on imports of high-value Chinese components, like batteries, would disincentivize domestic battery production and create enduring dependency on access to imported Chinese batteries. Moreover, any framework for investment must consider the full supply chain to illuminate chokepoints China controls or could exploit upstream, since, as critical mineral restrictions show, even small, low-value, commoditized components can throttle entire industries. And it should consider whether China's investment would substitute for or disadvantage U.S. or allied competitors bearing the cost of building secure domestic supply, which would entrench dependence.

Second, the U.S. government has revealed that China has prepositioned for offensive cyber attacks on U.S. power, gas, water, telecommunications, and transportation affecting tens of millions of Americans. For this reason, national security considerations should be a separate and overriding test from economic benefits when access to critical infrastructure, sensitive data, networks, or systems essential to public safety and national defense are implicated. In such cases, investment should be prohibited unless there are hard structural separations in governance and at the technical level, possibly including substitution with U.S. and allied approaches; when the outcome is unclear or contingent on corporate assurances, as it is in the report's TikTok stress test, the better approach is prohibition regardless of promised jobs, technology transfer, or lower costs.

These emphases are critical because compliance will be hard to secure over an investment's entire life, as the stress tests reveal, since incentives often run the other way for both American and Chinese companies. American firms can profit, for example, by hollowing out their own supplier base and growing dependent on Chinese inputs, as some U.S. automakers propose. Chinese firms, for their part, may never be made to comply fully with security mitigation, as the TikTok stress test shows. And the United States, as a free society bound by the rule of law, lacks the instruments China brings to bear on foreign investment, from significant state capacity and experience to the Party's reach inside private and state firms. Policymakers should therefore move cautiously and case by case by testing specific investments in key industries rather than adopting wholesale new approaches. Where allied investment is available in a given sector, it should be preferred. As the United States pursues "selective openness," the emphasis must fall on "selective" rather than "openness."





Stress Test 1 – Corporate Governance

Stress Test 1 — Corporate Governance

Corporate Governance for Chinese Direct Investment in the United States

By Meg Rithmire, Harvard Business School

National security concerns have been the most important factor limiting Chinese direct investment in the U.S. The Selective Openness framework takes seriously both those concerns and the need to address trade and technology imbalances. Some investments from China will be unacceptable because their benefits do not outweigh their risks. Nevertheless, some potential investments could benefit the United States if their terms are set prudently. We therefore propose a framework with policy templates for Chinese direct investment in the U.S. that allow flexibility based on risks and benefits. We also seek to establish a predictable set of regulatory measures that would enhance U.S. credibility in commercial transactions.

The Selective Openness framework proposes expanding the policy tools used to manage risks and increase the benefits of Chinese FDI by focusing on corporate governance mechanisms that go beyond traditional CFIUS proceedings. These mechanisms would provide stakeholders, including the U.S. public, with greater assurance that investments are safe, economically beneficial and subject to ongoing oversight. Measures ensuring transparency, continuous monitoring, supplier diversification, structural separation and enforcement would provide

a strong foundation for safe and productive Chinese FDI in the U.S.

A systematic corporate governance approach offers an effective form of risk management that can enable more flexible government oversight and monitoring while remaining responsive to market realities. Major banks and corporations operating in critical infrastructure sectors are already subject to regulatory regimes that combine traditional government oversight with internal corporate governance and risk management practices. The goal is to manage security concerns while preserving flexibility in complex commercial environments, similar to the approach the National Institute of Standards and Technology (NIST) takes toward corporate cybersecurity.¹³

This working group does not endorse a specific method for implementing the recommended corporate governance template for risk management; the details are too complex. Instead, we advocate an innovative policy approach and identify questions that implementation would need to address. By focusing on corporate governance, this stress test of the Selective Openness framework illustrates one possible path to implementation. It is designed to complement and augment the foreign direct investment risk management system anchored in the CFIUS process.

Current regulatory tools — including CFIUS review, export controls and entity lists — are largely reactive and applied inconsistently across sectors. They often lack robust, long-term enforcement mechanisms after investments are approved. As a supplement to help CFIUS advance desired economic and technological goals, proactive governance measures imposed as conditions of investment could provide structural

13 National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," February 26, 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>.

protections and oversight throughout an investment's life cycle.

The following is an outline of one such governance model. We recognize that specific governance structures and the intensity of scrutiny should be calibrated to sector sensitivity and the nature of the commercial relationship.¹⁴

I. Creating an Administrative Structure: A National Security Compliance Committee

Mitigation agreements negotiated during CFIUS review often involve the structural separation of sensitive assets and governance, U.S. personnel in oversight roles, and periodic operational reporting to ensure continuous monitoring of security-sensitive investments. Although these arrangements are necessarily case-specific and often opaque and confidential, their underlying principles — such as U.S. control over critical data and intellectual property, continuous oversight, and repeated disclosure — can be adapted more broadly if the U.S. seeks to attract Chinese investment while effectively mitigating national security risks.

Drawing on these principles, an illustrative administrative structure could take the form of a U.S. National Security Compliance Committee (NSCC), supported by strong governance structures, rigorous due diligence and proactive transparency requirements. Companies receiving investment from China, including wholly owned subsidiaries of Chinese companies, would be required to establish and maintain an NSCC with enforceable mandates designed to protect U.S. interests:

A. The NSCC Structure and Composition

- The NSCC must be based and staffed within U.S. operations, with limited remote participation by China-based personnel when necessary
- Its membership should include independent U.S.-based legal counsel with a national security clearance; cybersecurity professionals; compliance officers; and, when appropriate, independent U.S. board members with government or national security experience
- Committee members must undergo background checks and be U.S. citizens or permanent residents
- The NSCC must operate independently of the parent company's direction on national security matters, including data storage and transmission, oversight of relevant intellectual property, and interactions with critical infrastructure
- All deliberations must be documented and made available to U.S. regulators on request, in addition to being included in regular reports

¹⁴ These recommendations draw on a framework developed for U.S. companies doing business in and with China. See David Fagan and Meg Rithmire, "High Stakes: A Framework for Managing Geopolitical Risk," U.S. Chamber of Commerce, 2024, https://www.hbs.edu/ris/Publication%20Files/High-Stakes-A-Framework-for-Geopolitical-Risk-Management_ff45b547-9b38-4b39-9156-d7ae9c9159de.pdf; and National Cyber Security Centre, "Huawei Cyber Security Evaluation Centre," in *NCSC Annual Review 2021*, <https://www.ncsc.gov.uk/collection/ncsc-annual-review-2021/technology/huawei-cyber-security-evaluation-centre>.

B. The NSCC's Mandatory Authority

- The NSCC must have binding veto power over decisions involving:
 - The collection, retention or cross-border transmission of U.S. personal data
 - Access to U.S. critical infrastructure or integration with government systems
 - Research and development activities involving technologies identified on the Commerce Control List or the CFIUS critical technologies list
 - The hiring of personnel with access to sensitive systems, subject to background checks
 - Modifications to information technology architecture that affect data segregation
 - Partnerships with Chinese entities
- The NSCC must have authority to halt operations if national security risks cannot be adequately mitigated
- The NSCC must have a direct pathway for escalating threat reports to CFIUS and the FBI

C. Enforcement Mechanisms

- Annual certification to CFIUS that the committee maintains the required independence and authority
- Quarterly compliance reports subject to audits by U.S. government-approved third parties
- Whistleblower protections and financial incentives for employees who report committee failures to federal authorities

This structure would ensure that commercial pressure from a Chinese parent company cannot override national security considerations.

II. Continuous Monitoring

Continuous monitoring requirements would give U.S. authorities visibility into Chinese investment activities and help them detect threats before those threats materialize.

A. Real-Time Oversight Systems

- Automated monitoring of all cross-border data transmissions, with immediate alerts to the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) for unauthorized transfers
- Quarterly penetration testing by U.S. government-approved contractors to identify vulnerabilities
- Mandatory reporting to federal authorities within 24 hours of any cybersecurity incident, suspected espionage or contact by the Chinese government
- Annual comprehensive security audits, with results provided to CFIUS
- Continuous monitoring of employee activity for indicators of insider threats, with suspicious activity reported to the FBI

B. Compulsory Information Sharing, When Necessary

- Participation in sector-specific Information Sharing and Analysis Centers

- Quarterly threat briefings with relevant federal agencies, including the FBI, National Security Agency, CISA and Department of Defense
- Immediate disclosure of requests from the Chinese government for data, access or operational changes
- Cooperation with congressional oversight, including document production and testimony

III. Institutionalizing Cybersecurity, Supply Chain and, When Necessary, Structural Separation Requirements

An NSCC within a firm receiving Chinese investment would provide an institutional focal point for implementing supplier diversification principles and cybersecurity requirements. The governance framework would offer an enduring, iterative and adaptable means of ensuring that requirements are met and practices are adjusted in real time.

As noted in the stress test on cybersecurity and personal data controls, clear precedents exist for managing cyber risks. The NSCC would be responsible for overseeing cybersecurity and network segregation requirements. These could include any or all relevant elements of a cybersecurity template, such as:

- Complete physical and logical separation of U.S. operations from the Chinese parent company's networks
- Exclusive storage of all U.S. personal data on U.S.-based servers in secure facilities with physical access limited to U.S.-based personnel
- No network connectivity between U.S.-based and China-based systems; all communications must use secure, monitored channels
- Separate information technology infrastructure, email domains, collaboration platforms and cloud services using only U.S.-based providers
- A prohibition on remote access to U.S. systems from outside the United States
- Administration of all information technology systems by U.S.-based personnel who have undergone background checks
- Required use of U.S. government-approved encryption standards for all data at rest and in transit
- Regular vulnerability assessments and compliance audits by CISA-approved contractors

The NSCC would also monitor and phase in supply chain and supplier diversification requirements:

- Different industries will require different levels of upstream and downstream supplier diversity. The NSCC would draft and share diversification plans and ensure periodic review of progress toward phased goals.
- Although the NSCC structure would vary by firm and sector, periodic reporting and planning would provide industrywide transparency into diversification plans. This would set market expectations and provide benchmarks and accountability.

In sectors involving sensitive critical infrastructure or critical technologies, or where U.S. intellectual property and technical know-how could be exposed, governance frameworks could impose more stringent structural separation requirements.

A. Corporate Structure Requirements

- U.S. operations must be established as a legally separate entity with independent governance
- The board of directors must have a majority of independent U.S. directors with a fiduciary duty to protect U.S. national security
- The chief compliance officer must be a U.S. person who reports directly to independent board members and provides annual certification to CFIUS
- The parent company's access to U.S. operations must be limited to financial information; operational decisions must remain with the U.S. entity
- Requests by the parent company for information beyond financial data must be reported to federal authorities within 48 hours
- Employment contracts for all U.S.-based employees must explicitly prohibit responses to requests from the Chinese government

B. Restricted Information Sharing

- Formal protocols must strictly limit the information that may be shared with the parent company
- All technology transfers to the parent company require advance approval from the NSCC and notification to the Commerce Department
- The sharing of source code, algorithms, customer data, and research and development information is presumptively prohibited
- Any sharing of technical information automatically triggers an export control or bulk-data review

IV. Regulatory Oversight and Access

The NSCC would serve as the primary point of contact between the U.S. government and firms receiving Chinese investment, enabling better cooperation, documentation and regulatory oversight. Clear cooperation requirements and documentation standards would facilitate information sharing and build trust.

If the committee structure succeeds, transparency and periodic reporting could reduce alarm and ad hoc scrutiny from government bodies, such as congressional select committees and state attorneys general. At a minimum, the NSCC would provide a point of contact for responding to appropriate scrutiny from these groups.

A. Mandatory Cooperation Requirements

- Grant federal agencies, including the FBI, CISA, Commerce Department and Treasury Department, unannounced inspection rights for all facilities, systems and records
- Allow relevant federal agencies real-time access through application programming interfaces to monitor network traffic and data flows
- Maintain detailed audit logs of all system access, data queries and administrative actions for at least seven years

- Establish a whistleblower hotline directly to the FBI for employees to report security concerns or pressure from the Chinese government
- Provide legal protections and financial rewards for employees who report violations to federal authorities

B. Documentation Standards

- Document all NSCC decisions, security protocols and risk assessments
- Issue regular compliance reports in a standardized format suitable for automated analysis by federal agencies
- File incident reports for security events, suspicious activity or anomalous data access patterns
- Provide quarterly certifications by the CEO and chief compliance officer attesting to compliance, with personal liability for false statements

These safeguards would create physical and legal barriers to data exfiltration and technology transfer while providing U.S. authorities with the oversight tools needed to detect and respond to threats.

V. Conclusion

The corporate governance stress test shows how a process for managing risks from Chinese FDI could work. Critically, the Selective Openness framework requires innovation in U.S. governance processes. It offers a flexible but authoritative framework that protects U.S. interests while enabling practical implementation. A carefully designed, iterative NSCC structure could provide meaningful and ongoing transparency, incorporate supplier diversification requirements when appropriate, support internal and external oversight, and facilitate structural separation when necessary. Implementation details would be modified to suit specific purposes.

This corporate governance structure also offers important advantages by shifting part of the burden of risk mitigation from the U.S. government to the firms themselves.

First, governance requirements can serve as an important deterrent. Even when calibrated to sector sensitivity, stringent transparency, compliance and oversight obligations would make U.S. investments less attractive to firms unwilling to accept scrutiny — particularly those with malign intentions. Significant penalties and personal liability for executives would further discourage conduct that could endanger U.S. national security.

Second, this model shifts aspects of enforcement and accountability to firms without imposing overly rigid regulatory mandates. As with sanctions and export control compliance systems, clear personal liability provisions and mandatory internal compliance processes would give firms incentives to internalize their security obligations. Government inspection rights, coupled with documentation requirements, would enable systematic verification rather than reliance solely on ad hoc self-reporting.

Third, a governance-based framework allows policy flexibility. Oversight requirements can be strengthened or adjusted in response to evolving geopolitical dynamics, changing sector risks or technological developments. They could also serve as a baseline for negotiating coordinated safe-investment frameworks with allies and partners pursuing similar Selective Openness approaches.

The Selective Openness framework acknowledges that Chinese entities operate within a fundamentally different legal and political environment, in which state authorities may compel firms to act contrary to U.S. interests. The proposed NSCC framework —

combining strong governance, comprehensive due diligence, structural safeguards and proactive transparency – would create mechanisms through which Chinese investors and their U.S. partners can continuously monitor, communicate and fulfill their duties as responsible stewards of U.S. data, technology and economic resilience.

Although governance structures should be tailored to specific firms, sectors and transaction types, our approach demonstrates that deliberate corporate governance design can effectively manage many national security concerns by institutionalizing security-conscious decision-making and maintaining transparent, auditable operational processes.

Stress Test 2 – Cybersecurity

Stress Test 2 – Cybersecurity

Cybersecurity and Personal Data Controls for Chinese Direct Investment in the U.S.

By Peter Cowhey, UC San Diego School of Global Policy and Strategy

Every major sector of the global economy depends on computing, software, and data. As a result, Chinese direct investment in the United States raises concerns about cybersecurity and the protection of personal data. The Commerce Department's January 2025 rule banning Chinese "connected car" technology in the United States illustrates the breadth of those concerns.¹⁵ Examining how the main report's selective openness framework could manage cyber risk in U.S. EV manufacturing provides a useful test case for addressing broader policy challenges. This study examines Tesla's data arrangements in China and TikTok's agreements with the U.S. government as potentially instructive case studies for designing cybersecurity safeguards governing Chinese investment in U.S.-based manufacturing.

Any restrictions on cybersecurity and data flows involving Chinese operations in the United States require careful balancing with U.S. trade and investment policy. The United States has long advocated trade rules that permit cross-border data flows and allow companies to locate and configure data infrastructure freely around the world. Restricting Chinese investment therefore requires treating China as a country presenting distinctive security risks. There is ample precedent for doing so.

Two broad approaches are available for addressing data security and cybersecurity risks. Both approaches are consistent with the corporate governance principles embedded in the selective openness framework because cybersecurity and data protection must be integrated into core business operations.

- **Banning Core Products:** Ban core products and services that pose significant cybersecurity risks that cannot readily be mitigated and that provide little or no economic benefit to the United States. When weighing bans, policymakers should discern if the ban significantly advances an overall security goal.
- **Managing Products and Technologies:** Manage products and technologies that provide substantial economic benefits but pose cybersecurity or data protection risks through structural separation and supplier diversification. Measures may include restricting cross-border data flows, in whole or in part, and imposing targeted software and hardware requirements. Depending on the investment's structure and transparency obligations, continuous monitoring and specialized enforcement rules can reinforce these safeguards while preserving a viable business.¹⁶

¹⁵ Perhaps most dramatically, Pirelli, an Italian tire maker with a majority Chinese investor, has to restructure its corporate holdings to put its "connected tire" division under a new ownership umbrella. Stephen Wilmot, *The Car Industry is Racing to Replace Chinese Code*, *Wall Street Journal*, February 5, 2026.

¹⁶ Restrictions on data flows do not have to be all or nothing. The "commercial contract" model in U.S.-EU data flows allows considerable cross-border data movement even when the EU and the US repeatedly failed to reach a sustainable agreement on

For EV producers, data gathering is critical for several reasons. For one, a good deal of the value added, and therefore the profit margin, from EVs is in the software/digital control stack of the car. EVs are rightly characterized as computers with wheels. This is why tensions are even growing between American companies, such as GM and Apple, about their respective roles in software systems (e.g., CarPlay and mapping) and the revenues derived from them.

Consider the possibility of Chinese EV foreign direct investment (FDI) in the U.S. Assuming that Chinese EV production in the U.S. might sufficiently alleviate concerns about unfair competition, security concerns would remain, just as China had expressed concerns over Tesla's cars manufactured in Shanghai.

Because of security risk issues, governments worry about everything ranging from nuanced data collection to possible "bugs" in software and hardware (such as specialized semiconductors in cars). But Tesla in China and TikTok's continuing operation in the U.S. demonstrate the utility of a risk management approach. These two cases illustrate the importance of structural separation of sensitive operations, transparency in risk management controls, and diversification of sourcing, with the digital architectural principle of "modularity" proving especially significant.

I. The Tesla Bargain in China

For several years, Tesla faced Chinese government concerns over how it collected, stored and used data.¹⁷ In May 2021, Tesla responded by establishing a data center in China to comply with regulations requiring that data be stored locally. Even after opening the data center, however, Tesla vehicles remained barred from military bases and other sensitive government facilities because of security and privacy concerns.

In April 2024, Elon Musk met with Premier Li Qiang to negotiate an agreement. According to Bloomberg, the review examined how Tesla vehicles collected sensitive personal information, whether drivers could disable data collection, and whether Tesla would anonymize sensor data capturing license plates and faces.

The agreement also created a commercial incentive for Tesla to adopt Baidu's mapping software, Baidu being one of 20 Chinese firms permitted by the government to use higher-resolution mapping data for commercial purposes. The arrangement assured Chinese regulators that vehicle data would remain in China and be processed through software that complied with the country's security requirements.

Tesla's incentive was equally straightforward. Until then, Tesla had relied primarily on vehicle cameras and lower-quality mapping data. By adopting the higher-quality Baidu system, Tesla in return received

data privacy on certain highly controversial issues. Data continued to flow under industry specific "contracts," created in consultation between government and industry, that spelled out the safeguards to be applied. More generally, much of world commerce operates through "private governance" arrangements, such as technical standards and safety certifications.

¹⁷ Sources for this account include Agencia EFE, "Tesla Clears China's Data Security Requirements, Moves Closer to Self-Driving Tech Rollout," *EFE Noticias*, April 29, 2024, <https://efe.com/economia/2024-04-29/tesla-clears-chinas-data-security-requirements-moves-closer-to-self-driving-tech-rollout/>; Bloomberg, "As Musk Visits China, Tesla Wins Key Data Security Clearance," *Bloomberg*, April 29, 2024, <https://www.bloomberg.com/news/articles/2024-04-29/as-musk-visits-china-tesla-wins-key-data-security-clearance?embedded-checkout=true>; Keith Bradsher and Jack Ewing, "Tesla Reaches Deals in China on Self-Driving Cars," *New York Times*, April 29, 2024, <https://www.nytimes.com/2024/04/29/business/elon-musk-tesla-china-full-self-driving.html>; and "Tesla Says

approval to deploy its supervised Full Self-Driving system, with a human still watching, for a \$99/month upgrade option. In exchange, Baidu received a valuable endorsement of its system by a global auto producer.

The mapping-system substitution illustrates how supplier diversification can reduce security risks in digital systems. This is possible because modern digital systems rely on modular architectures that allow components from multiple suppliers to be integrated, modified and documented.¹⁸ For example, Microsoft software incorporates substantial amounts of open-source code developed outside the company. Modularity is neither seamless nor cost-free, but it is very frequently a viable option. U.S. and European automakers are already engineering modular swap-outs in their current systems for security reasons.¹⁹

The Tesla case, including the high-level political engagement, could be a valuable template for Chinese EVs seeking entry into the U.S. If BYD sought to establish manufacturing facilities in the U.S., it could offer to use U.S.-sourced systems for mapping data as well as localized data storage and computing facilities. Data protection could be further strengthened if, as some experts believe, data could be tagged to trace any transfer across U.S. borders.

Even so, this approach may not satisfy American critics of personal data protection and security

risks involving Chinese products. Indeed, the Biden administration issued a new rule in its closing months on the movement of personal data of U.S. citizens to locations outside America that could prove quite restrictive for China. The underlying executive order issued by President Biden that directed the creation of these rules was one of the few such orders that survived the transition, with the Department of Justice (DOJ) finalizing the rules in early 2025.²⁰

How the rules will ultimately be implemented remains uncertain. But one must assume that any data-intensive investment that involves routine data transfers to China would be impacted. These restrictions may reduce Chinese firms' willingness to invest in affected sectors where strict data localization is not feasible. Still, the Trump administration's handling of data and security issues concerning TikTok suggests it may be amenable to a more flexible approach, as discussed below.

II. TikTok as a Precedent for Chinese FDI in EVs in the U.S.

TikTok's experience in the United States provides a useful precedent for how the Trump administration might approach Chinese investment in other sectors. ByteDance entered the U.S. market through its 2017 acquisition of the American video app Musical.ly. Although President Trump expressed skepticism,

It Has Established a Data Center in China," *Data Center Dynamics*, April 29, 2026, <https://www.datacenterdynamics.com/en/news/tesla-says-it-has-established-a-data-center-in-china/>.

18 A clear exposition of modular design in software is Sanjoy Kumar Malik, "A Gentle Guide to Modular Software Design," LinkedIn, posted October 12, 2024.

19 As the robotics stress test in this report notes, even more sophisticated applications of modularity appear feasible. NVIDIA's Jetson software platform, for instance, is a viable substitute for Chinese platforms such as Tencent's TAIROS across many core robotics functions.

20 Justice Department Implements Critical National Security Program to Protect Americans' Sensitive Data from Foreign Adversaries. (2025, April 11). Justice.gov. (<https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive>)

the courts declined to block the transaction. TikTok debuted at scale and boomed.

Critics argued that TikTok could collect extensive information on U.S. users, including military personnel, and share it with the Chinese government. Such information could be exploited in three principal ways: (1) coercion or blackmail; (2) collection of sensitive location and behavioral data; and (3) manipulation of public opinion through algorithmic content recommendations.

These accusations led Congress to set a deadline, signed into law by President Biden, for TikTok to either exit the U.S. market or be sold to U.S. owners.

TikTok sued, claiming violations of the free speech rights of its users. TikTok also deployed a skilled political and public relations campaign. Given its popularity, particularly among younger cohorts, this was an important political factor that caught the attention of the Trump political apparatus.

To address concerns that it would share data with the Chinese government, TikTok struck a deal with Oracle to store its U.S. data. Oracle, whose chairman and chief technology officer is Larry Ellison, became responsible for storing U.S. user data. The arrangement mirrored Tesla's decision to establish a data center in China to satisfy Chinese regulatory requirements.

Ultimately, the Trump administration permitted TikTok to continue operating in the United States under a restructured ownership arrangement. Oracle, the

private hedge fund Silver Lake Management, an Abu Dhabi investment group, and smaller investors gained an 80.1% share of a U.S. TikTok corporation. Notably, ByteDance retained a 19.9% ownership stake, despite Congress' original intent that TikTok either divest or exit the U.S. market. Moreover, TikTok reportedly agreed to pay a \$10 billion brokering fee to the U.S. Treasury.²¹

The agreement also imposed additional safeguards. To mitigate security risk, U.S. TikTok must use Oracle data storage and undergo technical monitoring of TikTok's codebase. The U.S. entity received a perpetual license to TikTok's code. The arrangement suggests that the Chinese government only agreed to the TikTok deal because IP ownership of key code remains in the hands of ByteDance. Oracle was authorized to modify algorithms after retraining them exclusively on U.S. users' data. The data storage and algorithm retraining represent a limited form of structural separation and supplier diversification of the technical core of TikTok to resolve its cybersecurity issues.

Yet TikTok still poses an unusual challenge even under this restructuring. TikTok's rapid growth was driven in large part by recommendation algorithms that identified potential users based on both the content of images and users' engagement with them, rather than on the social network of the person posting the content. Constantly refining this code is essential and complex work. Initially, Software engineering was conducted primarily in China, although additional input came from centers in TikTok's Singapore headquarters

21 Miriam Gottfried and Armin Ramkumar, "Trump Administration Set to Receive \$10 Billion Fee for Brokering TikTok Deal," *Wall Street Journal*, March 13, 2026. The financial terms are also reportedly very favorable to ByteDance. See also Bloomberg News, "ByteDance Emerges from TikTok Saga with 'Major Win' on U.S. Access," *Bloomberg*, January 2026; and Rafe Rosner-Uddin, Demetri Sevastopulo, and Alex Rogers, "TikTok Algorithm to Be Overseen by Oracle in Trump Deal," *Financial Times*, September 22, 2025.

and in Silicon Valley.²²

The central policy questions concern corporate governance and software oversight. As the Selective Openness framework argues, higher-risk investments require correspondingly stronger governance arrangements of a joint venture. In this case, the CEO of ByteDance holds a board seat and the remaining six seats are held by U.S. directors. However, much of the key leadership of TikTok consists of ByteDance global executives with Singaporean citizenship. Moreover, ByteDance, not the U.S. TikTok entity, controls marketing and advertising—two factors which influence algorithm designs. Although Oracle controls the U.S. algorithm, important questions remain about the possible role of ByteDance’s software engineering team working on key algorithms.²³

These ambiguities go to the heart of whether the deal addresses American officials' principal concern: political manipulation of public opinion by TikTok. That is precisely why our framework’s corporate governance approach would require extensive transparency, continuous monitoring and rigorous security audits of TikTok’s content and data systems.

III. Conclusion

The Tesla and TikTok cases demonstrate that it is possible to establish safeguards for certain categories of U.S. personal and geolocation data that both address the Trump administration's security concerns and preserve the economic benefits of Chinese investment in the United States. Indeed, in February 2026, the Trump administration paused implementation of certain additional Commerce Department digital security rules.²⁴

Applied to Chinese EV investment, the TikTok model would broadly parallel the requirements China imposed on Tesla. The U.S. approach, however, could also require that the investment take the form of a joint venture, with more extensive structural separation and modular diversification of Chinese digital technology.²⁵ Additional requirements could include U.S. content thresholds, technology transfer and workforce training. Because some industry analysts estimate that Chinese manufacturers could profitably export EVs to the United States even under tariffs of 50%, they could likely absorb significant compliance costs associated with U.S. foreign direct investment requirements while remaining commercially competitive.

More broadly, the Tesla and TikTok cases reinforce the central premise of our Selective Openness framework. Cybersecurity and data protection concerns do not necessarily require categorical restrictions on Chinese investment. Rather, they suggest that national security and economic objectives can often be advanced

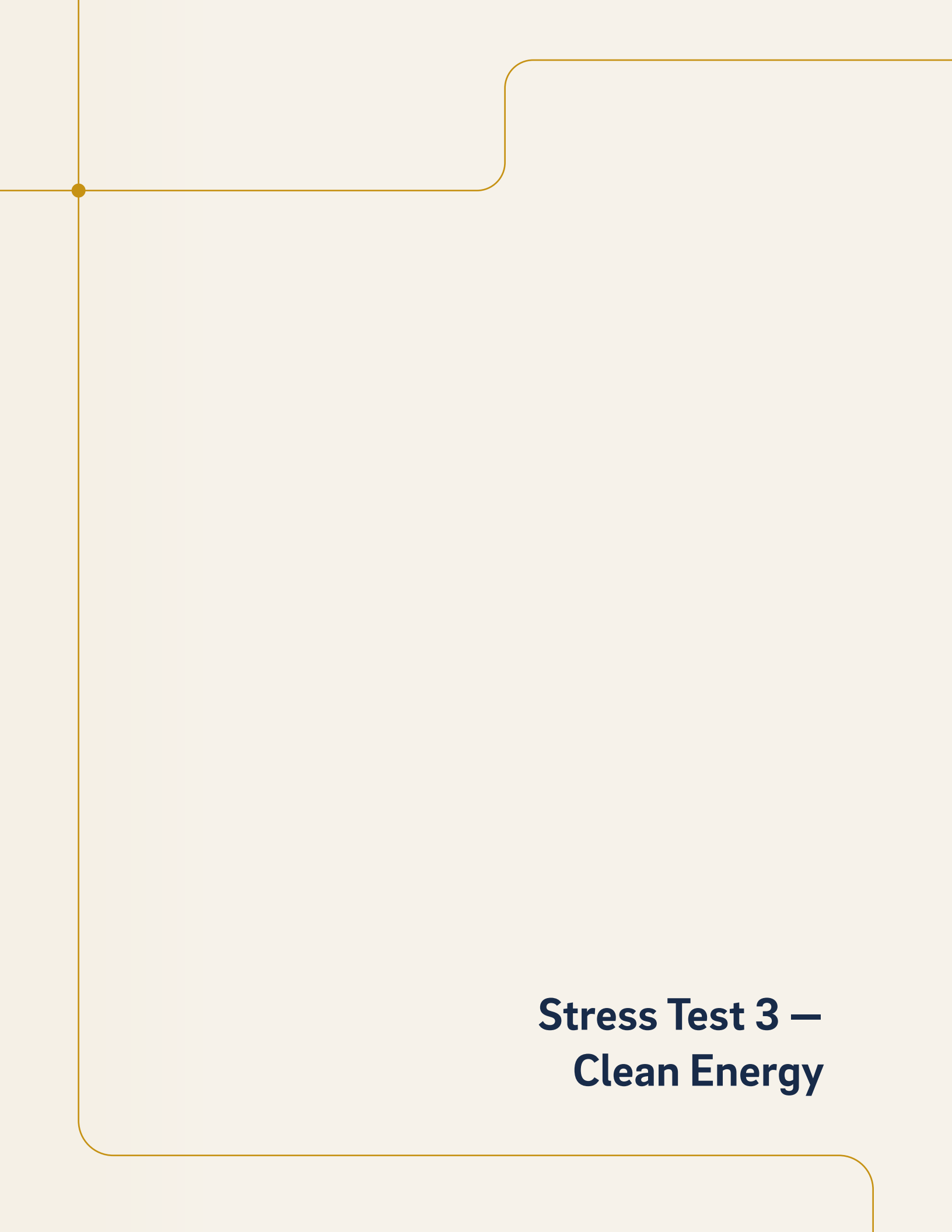
22 Kelley Cotter, "TikTok's New Owner Puts App's Algorithm in the Spotlight—A Social Media Expert Explains How the 'For You' Page Works," *The Conversation*, September 22, 2025, <https://theconversation.com/>.

23 "The Cloud Has Lifted—TikTok Is Back," March 26, 2026, *Bloomberg Technology*.

24 The ban on routers from countries of concern later proceeded. Alexander Alper, "Exclusive: Trump Pauses China Tech Bans Ahead of Xi Summit," *Reuters*, February 12, 2026.

25 Adrian Leung, "Ford, Xiaomi Deny Reports of U.S. EV Joint Venture Talks," *CarNewsChina*, February 1, 2026, <https://carnewschina.com/2026/02/01/xiaomi-and-ford-deny-reports-of-electric-vehicle-joint-venture-talks-in-the-united-states/>.

simultaneously through carefully designed governance mechanisms, including structural separation, supplier diversification, data localization where appropriate, and robust transparency and oversight requirements. The challenge for policymakers is not simply whether to permit or prohibit investment, but how to design institutions that manage risk while preserving the economic benefits of Selective Openness.



Stress Test 3 — Clean Energy

Stress Test 3 – Clean Energy

Chinese Investment in U.S. Energy and Automotive Sectors

By Michael Davidson, UC San Diego School of Global Policy and Strategy and Jacobs School of Engineering

Jonas Nahm, Johns Hopkins University School of Advanced International Studies

Clean energy and electric vehicle manufacturing are sectors where the United States most urgently needs to close a capability gap in global frontier manufacturing; they are also where Chinese firms have the most to offer as potential partners. China controls the overwhelming majority²⁶ of global lithium-ion battery production, dominates solar panel manufacturing²⁷ and has built vertically integrated EV supply chains that run from raw material processing²⁸ to finished vehicles. These advantages reflect genuine process expertise, co-located supply ecosystems and the competitive pressure of a domestic market that has driven relentless cost reduction and quality improvement. American firms cannot simply replicate these capabilities through domestic investment alone on any relevant timescale.

This creates a policy challenge distinct from sectors where the primary question is whether to permit Chinese engagement. In clean energy, some form of engagement is already deeply embedded, including through licensing, joint ventures and wholly foreign-owned subsidiaries. The question is whether it can be structured to build American industrial capacity rather than simply providing Chinese firms access to the U.S. market.

This stress test applies the Selective Openness framework to that question. It proceeds in four parts: a characterization of the strategic landscape; an assessment of sector-specific risks and benefits; an application of the three investment models to distinct segments of the clean energy value chain; and complementary U.S. policy actions that would make structured Chinese engagement more productive.

I. Strategic Landscape

China's position in clean energy supply chains reflects decades of coordinated industrial policy combined with the learning effects of producing at extraordinary scale. Chinese firms now account for over 80 percent²⁹ of global lithium-ion battery manufacturing capacity, a comparable share of solar panel production³⁰ and dominant

26 Teo Lombardo et al., "Global Battery Markets Are Growing Strongly—and So Are the Supply Risks," International Energy Agency, February 13, 2026, <https://www.iea.org/commentaries/global-battery-markets-are-growing-strongly-and-so-are-the-supply-risks>.

27 International Energy Agency, "Executive Summary," in Solar PV Global Supply Chains, July 2022, <https://www.iea.org/reports/solar-pv-global-supply-chains/executive-summary>.

28 U.S. Energy Information Administration, "China Dominates Global Trade of Battery Minerals," May 14, 2025, <https://www.eia.gov/todayinenergy/detail.php?id=65305>.

29 Lombardo et al., "Global Battery Markets."

30 International Energy Agency, "Executive Summary."

positions in the upstream processing of critical minerals³¹. In electric vehicles, Chinese firms have achieved levels of vertical integration³² and cost performance³³ that no U.S. or allied competitor can currently match.

The United States has moved to build its own clean energy industrial base. These efforts, however, have been highly dependent on the Inflation Reduction Act (IRA) and associated programs. These programs have generated mixed results³⁴ due to reversals and shortening³⁵ of policy support. Announced investments have been substantial, but many projects have stalled, scaled back or encountered supply chain constraints that trace directly back to Chinese upstream dominance. New restrictions on foreign entities³⁶, including Foreign Entity of Concern (FEOC), Prohibited Foreign Entities (PFE) and Material Assistance Cost Ratios (MACR), enhanced under the One Big Beautiful Bill Act, further temper enthusiasm and prospects for U.S. manufacturing.

The gap between U.S. industrial ambitions and domestic manufacturing capacity remains wide and is unlikely to close quickly. Chinese firms are already present in the U.S. automotive and clean energy sectors through a variety of investment structures. Examples include the Ford-CATL licensing arrangement in Michigan,³⁷ the Illuminate USA joint venture in Ohio,³⁸ Jinko Solar's³⁹ former majority-owned manufacturing facility in Florida, and Gotion's battery plant in Illinois.^{40,41}

31 U.S. Energy Information Administration, "China Dominates Global Trade."

32 Paolo Gerbaudo, "The Electric Vehicle Developmental State," *Phenomenal World*, February 27, 2025, <https://www.phenomenalworld.org/analysis/byd/>.

33 Noah Barkin et al., "Why Are Chinese EVs So Cheap?," Rhodium Group, June 11, 2025, <https://rhg.com/research/why-are-chinese-evs-so-cheap/>.

34 Clean Investment Monitor, "US Q4 2025 Update," February 19, 2026, <https://www.cleaninvestmentmonitor.org/reports/clean-investment-monitor-us-q4-2025-update>.

35 E2, "Clean Economy Works: December and 2025 Year End Analysis," February 2026, <https://e2.org/reports/clean-economy-works-2025-year-end-analysis/>.

36 Tax Law Center at NYU Law, "Treasury Releases First Round of Prohibited Foreign Entity Guidance," December 19, 2025, <https://taxlawcenter.org/blog/treasury-releases-first-round-of-prohibited-foreign-entity-guidance>.

37 Patrick George, "Ford's Affordable EV Comeback Starts Here. But Not Without Controversy," *InsideEVs*, June 23, 2025, <https://insideevs.com/news/763490/ford-blue-oval-park-lfp-preview/>

38 Illuminate USA, "A New Era of Manufacturing: Pataskala's Illuminate USA Starts Solar Panel Production," February 18, 2024, <https://illuminateusa.com/press/a-new-era-of-manufacturing-pataskalas-illuminate-usa-starts-solar-panel-production/>.

39 JinkoSolar, "Solar + Storage from One Company," accessed August 13, 2026, <https://jinkosolar.us/>.

40 Tim Levin, "Ford's Affordable EV Comeback Starts Here. But Not Without Controversy," *InsideEVs*, June 16, 2025, <https://insideevs.com/news/763490/ford-blue-oval-park-lfp-preview/>; Illuminate USA, "A New Era of Manufacturing: Pataskala's Illuminate USA Starts Solar Panel Production," February 1, 2024, <https://illuminateusa.com/press/a-new-era-of-manufacturing-pataskalas-illuminate-usa-starts-solar-panel-production/>; JinkoSolar US, "Jacksonville," accessed July 16, 2026, <https://jinkosolar.us/jax/>; Nora Eckert, "Michigan AG Asks Chinese Battery Maker Gotion to Return \$23.7 Million after Defaulting on US Plant," *Reuters*, January 30, 2026, <https://www.reuters.com/world/china/michigan-ag-asks-chinese-battery-maker-gotion-return-237-million-after-2026-01-30/>.

41 David Shepardson, "Michigan AG Asks Chinese Battery Maker Gotion to Return \$23.7 Million after Defaulting on US Plant," *Reuters*, January 30, 2026, <https://www.reuters.com/world/china/michigan-ag-asks-chinese-battery-maker-gotion-return-237-million-after-2026-01-30/>.

II. Sector-Specific Risks and Benefits

A. Benefits

The potential benefits of structured Chinese engagement are real. China's manufacturing process expertise is not easily acquired through domestic investment or licensing alone. Chinese partners can accelerate U.S. battery manufacturing capability, expose workers and firms to production techniques⁴² refined at scale and create demand for local supplier networks that would not otherwise exist. Localization may represent the most significant contribution Chinese FDI can make to the U.S. economy, much as Tesla localized approximately 95% of its supply chain in Shanghai within three years (2019–22).

Currently, the United States is experiencing a rapid expansion of battery manufacturing capacity, mostly for grid-scale energy storage. Yet at current trajectories of EV adoption and battery manufacturing investment, the alternative to structured engagement with Chinese firms is unlikely to be a thriving domestic sector. Instead, it risks widening America's capability gap and prolonging dependence⁴³ on Chinese imports of critical batteries, components, and materials.

B. Risks

Challenges for Selective Openness regarding clean energy manufacturing center on three distinct concerns: strategic supply chain dependency,⁴⁴ particularly in upstream inputs like cathode materials, mineral processing and battery components where Chinese dominance is most pronounced⁴⁵; the question of whether Chinese investment genuinely transfers manufacturing capability or reproduces Chinese supply chains on American soil with U.S. workers as assemblers rather than manufacturers; and data security/privacy issues related to control and the operation of digital equipment (an issue common to the other sectoral stress tests and discussed in greater detail in the cybersecurity paper).

There are also competitive dynamics that the framework must take seriously. The Fuyao case⁴⁶ — a Chinese

42 Jonas Nahm, "America Has an Edge over China. Why Won't We Use It?," *New York Times*, February 24, 2026, <https://www.nytimes.com/2026/02/24/opinion/china-america-manufacturing-ai.html>.

43 Noah Gordon and Stephen G. Gross, *Winning the Battery Race: How the United States Can Leapfrog China to Dominate Next-Generation Battery Technologies* (Washington, DC: Carnegie Endowment for International Peace, October 2024), <https://carnegieendowment.org/research/2024/10/winning-the-battery-race-how-the-united-states-can-leapfrog-china-to-dominate-next-generation-battery-technologies>.

44 International Energy Agency, "Beyond NMC Batteries: Supply Chain Issues for Emerging Battery Technologies," in *Global Critical Minerals Outlook 2025*, May 2025, <https://www.iea.org/reports/global-critical-minerals-outlook-2025/beyond-nmc-batteries-supply-chain-issues-for-emerging-battery-technologies>.

45 U.S. Department of Energy, *Four-Year Review of Supply Chains for the Advanced Batteries Sector* (Washington, DC: U.S. Department of Energy, December 2024), <https://www.energy.gov/sites/default/files/2024-12/20212024-Four%20Year%20Review%20of%20Supply%20Chains%20for%20the%20Advanced%20Batteries%20Sector.pdf>.

46 Gavin Bade, "The Chinese Factory That Opened in the U.S. and Clobbered Its Rivals," *Wall Street Journal*, February 24, 2026, <https://www.wsj.com/business/tariffs-china-trump-trade-4495c2a4>.

automotive glass manufacturer that took over a former GM plant in Dayton, Ohio and steadily outcompeted a unionized domestic rival through pricing — illustrates what happens when Chinese investment achieves domestic market dominance without transferring meaningful capability, such as diversifying a supply chain. Fuyao employs thousands of Ohio workers and is, by conventional measures, a successful investment. It has injected new dynamism into the industry and may ultimately expand the overall market for automotive glass, benefiting firms beyond Fuyao itself. But Vitro, the displaced competitor, is unionized, pays higher wages and has seen its volume collapse without offsetting benefits to the local production supply system. In sectors identified as critical to national security, investment screening that focuses only on espionage risk and misses structural competitive dynamics may fail to protect the broader industrial base the policy is intended to strengthen.

III. Applying the Three Investment Models

The Selective Openness framework identifies licensing, joint ventures and wholly foreign-owned enterprises as the primary investment modes. Each warrants different governance requirements calibrated to its risk profile and realistic learning potential.

A. Licensing

Licensing, exemplified by the Ford-CATL arrangement,⁴⁷ is the most appropriate structure for technology acquisition in battery chemistry and manufacturing processes where U.S. firms require rapid capability development without equity entanglement. Its principal limitation⁴⁸ is that licensing agreements typically restrict what a licensee can access, modify or learn — allowing firms to operate a technology without the process knowledge needed to understand, troubleshoot or independently improve it. The gap between possessing technical specifications and mastering production processes tends to widen over time as the licensor advances and the licensee remains dependent on contractual access to keep pace.

Governance requirements for licensing should therefore focus on technology domestication: provisions requiring that licensing arrangements include genuine access to process knowledge rather than merely operational rights; contractual obligations on licensors to disclose upgraded roadmaps and extend those rights to future process improvements; and milestones requiring licensees to demonstrate growing independent capability over defined timelines. The goal is a licensing relationship with a built-in pathway toward technological independence rather than continued dependence. FEOC determinations should assess genuine operational control⁴⁹ rather than applying ownership thresholds mechanically. Arrangements that appear arm's-length on paper can recreate

47 Levin, "Ford's Affordable EV Comeback."

48 Gary Gereffi, John Humphrey, and Timothy Sturgeon, "The Governance of Global Value Chains," *Review of International Political Economy* 12, no. 1 (2005): 78–104, <https://doi.org/10.1080/09692290500049805>.

49 Abigail Hunter, "The Devil Is in the Details: Minerals, Batteries, and US Dependence on Chinese Imports," *Council on Strategic Risks*, May 30, 2025, <https://councilonstrategicrisks.org/2025/05/30/the-devil-is-in-the-details-minerals-batteries-and-us-dependence-on-chinese-imports/>.

deep dependencies through the terms of the license itself.

B. Joint Ventures

Joint ventures, exemplified by Illuminate USA⁵⁰, are best suited to manufacturing segments where co-location of personnel is necessary for genuine knowledge transfer. This is where learning happens through shared problem-solving rather than technology documentation, but the risks are correspondingly greater. Governance complexity, asymmetric learning,⁵¹ and the difficulty of unwinding integrated operations make joint ventures the highest-risk investment model in this sector.

Governance and contractual safeguards should therefore be more demanding than those applied to licensing arrangements. The requirements could encompass options such as allowable foreign ownership shares based on sector sensitivity, the possibility of distinct equity shares (e.g., limiting foreign ownership of land as in the case of Illuminate USA's Chinese partner), technology transfer milestones, vendor diversity requirements and local workforce development. The EU's proposed Industrial Accelerator Act⁵² — which conditions FDI approval for large investments in strategic manufacturing sectors on joint venture structures capped at 49 percent foreign ownership, IP licensing to the local entity and

minimum thresholds for local workforce employment and supply sourcing — offers a useful reference for how these conditions can be codified rather than negotiated on a case-by-case basis. The EU has also examined how to offset any cost advantages bestowed on Chinese FDI ventures from subsidies in their home country.

C. Wholly Foreign-Owned Subsidiaries

Wholly foreign-owned subsidiaries (WFOEs) like Jinko (prior to selling off its controlling stake) present the most complex governance challenge. Strategic decisions remain with the foreign parent and knowledge spillovers to U.S. firms depend heavily on local supplier ecosystems⁵³ that do not yet exist in most U.S. regions. The principal risk is that WFOEs reproduce Chinese supply chains⁵⁴ on American soil — importing components, processing and materials from Chinese affiliates — while employing U.S. workers at the assembly end of a value chain that remains Chinese.

Government requirements should focus on the central objective: building durable U.S. manufacturing capability through supply-chain diversification. The requirements could include local supplier development tied to any public subsidy specifying that WFOEs must create genuine demand for U.S. supplier networks rather than replicating upstream Chinese

50 Bloomberg, "How American Tax Breaks Brought a Chinese Solar Energy Giant to Ohio," *Crain's Cleveland Business*, October 2024, <https://www.craigslist.com/politics-policy/how-american-tax-breaks-brought-ohio-chinese-solar-energy-giant/>.

51 John H. Dunning, "The Eclectic (OLI) Paradigm of International Production: Past, Present and Future," *International Journal of the Economics of Business* 8, no. 2 (2001): 173–190, <https://doi.org/10.1080/13571510110051441>.

52 European Commission, Proposal for a Regulation Establishing a Framework of Measures for the Acceleration of Industrial Capacity and Decarbonisation in Strategic Sectors (Industrial Accelerator Act), COM (2026) 100 final (Brussels, March 4, 2026), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2026:100:FIN>.

53 U.S. Department of Energy, Four-Year Review.

54 Bloomberg, "U.S. Solar Factories Find Chinese Suppliers Indispensable," *Japan Times*, July 18, 2024, <https://www.japantimes.co.jp/environment/2024/07/18/energy/us-solar-factories-china/>.

dependencies, vendor diversity mandates with phased timelines and facility location restrictions for proximity to critical infrastructure. The principal metric should be supplier diversity — a range of non-Chinese suppliers — rather than total onshoring, which is neither feasible in the near term nor strictly necessary for resilience.

IV. What the Framework Requires to Work

The Selective Openness framework rests on the assumption that U.S. firms and workers have sufficient absorptive capacity⁵⁵ to benefit from structured Chinese engagement — that supplier ecosystems, workforce training and manufacturing capabilities are adequate to capture spillovers rather than simply providing market access. In clean energy, this assumption holds only partially.

The most acute structural gap is upstream⁵⁶. All three investment models face the potential for continued dependence on Chinese-controlled inputs, including cathode materials, mineral processing and auxiliary chemicals. Governance frameworks for Chinese FDI must be paired with affirmative investment in domestic and allied-country capacity for these inputs — analogous to what would be required in pharmaceuticals to rebuild active ingredient supply chains. There are already useful precedents in these sectors: for example, Illuminate USA, which has Chinese partner LONGi, chose to source polysilicon⁵⁷ from the UK instead of China. Vendor diversity is the achievable near-term target; genuine resilience requires sustained investment in materials and chemical manufacturing that the U.S. has allowed to atrophy.

A broader manufacturing capability gap⁵⁸ also limits what structured engagement can deliver. Recent evidence on AI deployment in Chinese factories suggests that China's edge in clean energy manufacturing reflects not only scale. Beyond scale, China has systematically integrated automation, robotics and digital production management into factory operations in ways that American manufacturers have not. If U.S. firms lack the digital manufacturing infrastructure to learn from Chinese partners, the knowledge transfer that joint ventures and WFOEs can in principle deliver will be constrained. As our Working Group recommendations emphasize, complementary government actions that maximize benefits from Chinese investment may be necessary. In this case, these could include federal and state investment in shared digital infrastructure, workforce training for advanced manufacturing and the connectivity of legacy equipment to modern data systems.

Data security and privacy concerns will be central to the energy equipment and automotive sectors as digitization and autonomous driving become key drivers of profit and product differentiation. While neglecting these facets will lead to costly resets later on when issues develop, banning outright Chinese investment and technology over data concerns unnecessarily hamstring the private sector. As discussed in the accompanying

55 Dunning, "Eclectic (OLI) Paradigm."

56 Elaine Dezenski and David Rader, "Unplugging Beijing," *Foundation for Defense of Democracies*, July 21, 2025, <https://www.fdd.org/analysis/2025/07/21/unplugging-beijing/>.

57 Third Way, "Securing US-China Engagements on Clean Energy Technology," accessed July 16, 2026, <https://www.thirdway.org/memo/securing-us-china-engagements-on-clean-energy-technology>.

58 Jonas Nahm, "America Has an Edge over China. Why Won't We Use It?"

cybersecurity paper, risk management practices exist for these kinds of investments, which could include data localization, algorithmic transparency and vendor diversity targets.

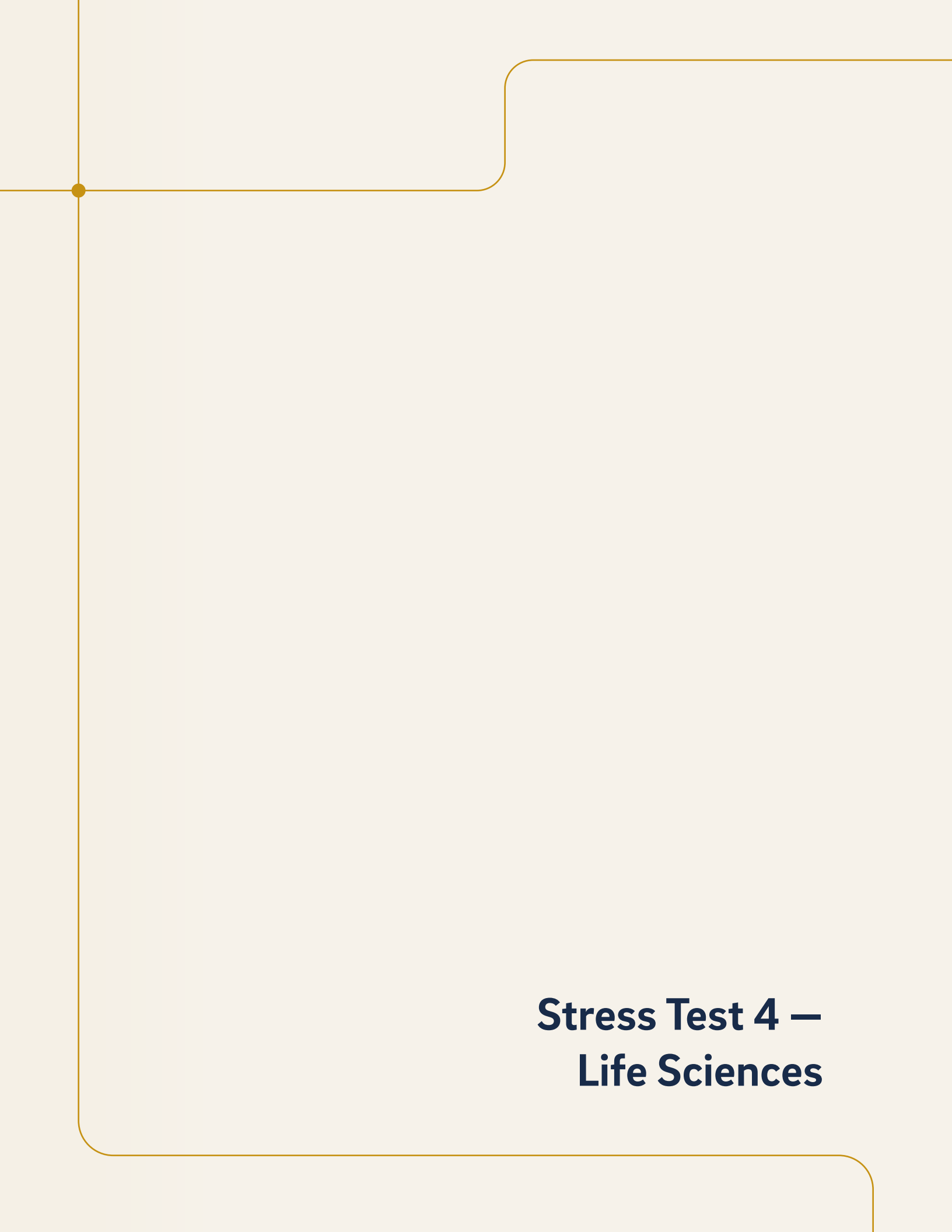
Finally, FEOC rules need refinement. Their current design can impose penalties on arm's-length arrangements that pose limited strategic risk while failing to distinguish between investment structures by their actual governance profile. A compliance pathway – analogous to CFIUS national security agreements – that grants firms FEOC eligibility through robust governance structures would reduce the chilling effect on investment without compromising meaningful oversight of genuinely risky arrangements.

Conclusion

Clean energy is among the more tractable sectors for the Selective Openness framework. Unlike more data-sensitive industries, the primary risks are structural rather than informational – supply chain dependency and the failure to transfer capability rather than the exposure of irreversible sensitive assets. And unlike sectors where Chinese dominance is still emerging, Chinese engagement is already well established: the task is to set its terms. A differentiated approach – more permissive for licensing with domestication requirements, more demanding for joint ventures and WFOEs with enforceable capability transfer milestones and supply chain diversification obligations – can provide framework for Chinese investment that builds American industrial capacity rather than substituting for it.

More broadly, the clean energy sector illustrates the central premise of the Selective Openness framework: the objective is not simply to regulate Chinese investment, but to ensure that it strengthens U.S. industrial capabilities. The key policy question is whether investment contributes to long-term capability formation through technology transfer, supplier diversification, workforce development and manufacturing know-how, rather than reinforcing structural dependence on Chinese production networks. When paired with complementary domestic investments and appropriately designed governance requirements, Selective Openness can help transform foreign investment from a source of vulnerability into a catalyst for rebuilding American manufacturing competitiveness.





Stress Test 4 – Life Sciences

Stress Test 4 – Life Sciences

Chinese Investment in U.S. Life Sciences

By Meg Rithmire, Harvard Business School

Tim Scott, Biocom California

The life sciences sector sits at the intersection of several of the United States' most strategically sensitive interests: genomic and health data, critical pharmaceutical supply chains, and the biomedical innovation ecosystem that underpins both national security and economic competitiveness. It is also a sector in which U.S.-China interdependence is unusually deep, making neither wholesale exclusion nor unrestricted access a workable policy approach.

This stress test applies the Selective Openness framework to the life sciences sector. It proceeds in four parts: (1) an overview of the strategic landscape, including the forms Chinese investment has taken and why they matter; (2) an assessment of sector-specific risks and benefits; (3) an application of three investment models – licensing, joint ventures, and wholly foreign-owned subsidiaries – across distinct segments of the life sciences ecosystem; and (4) complementary U.S. policy measures that could make Chinese investment in this sector more economically productive while mitigating associated risks.

I. Strategic Landscape

A. China's Established and Growing Life Sciences Advantages

China's life sciences sector has advanced substantially over the past decade. China's domestic ecosystem now supports innovation across the full spectrum of drug and medical-device development. State-directed industrial policies, such as the 13th and 14th Five-Year Plans (2016–2025), which explicitly prioritized life sciences and biotechnology as national research priorities, have contributed to growth in research and development. So have domestic reforms in the health sector, such as the expansion of the National Drug Reimbursement List in 2016.⁵⁹ Most recently, China's State Council issued a further round of policy incentives in December 2024 (Circular No. 53). These eliminated regulatory hurdles to market access for innovative drugs and devices, building on structural reforms first introduced in 2017.⁶⁰

59 People's Republic of China. *The Fourteenth Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Outline of Long-Range Objectives Through 2035*. Beijing: Xinhua News Agency, March 2021. English translation available via Creaders Network and NPC Observer.

60 State Council of the People's Republic of China. *Opinions on Strengthening the Whole-Chain Supervision of Innovative Drugs and Promoting the High-Quality Development of the Pharmaceutical Industry*. Circular No. 53. Beijing: State Council, December 30, 2024. See also Congressional Research Service, *China's Biotechnology Development: A Summary*, IF12560 (Washington, DC: Congressional Research Service, 2023).

The results are striking: By 2023, China had approved 89 new drugs — seven times as many as in 2018 — and accounted for 23 percent of the global innovative drug pipeline, with particular strength in biologics, precision medicine, and synthetic biology.⁶¹

B. Chinese Investment in U.S. Life Sciences: A Reality

Interdependence between China and the United States in life sciences is deep and bidirectional. The question is not whether Chinese firms are present in U.S. drug production, medical technologies, and related fields, but how that presence has been and could be managed. Chinese investment in U.S. life sciences has grown substantially over the past 15 years. It has taken three recurring forms, each of which raises distinct governance concerns.

1. Platform Technology and Data

The most nationally sensitive category of Chinese investment involves genomics platforms and health data infrastructure. BGI's acquisition of Complete Genomics in 2013 established an early precedent, securing CFIUS clearance while acquiring significant capabilities in genomic sequencing. WuXi AppTec's 2015 acquisition of NextCODE Health embedded a major Chinese firm in genomic analytics and bioinformatics. The 2017 iCarbonX investment in PatientsLikeMe later triggered CFIUS divestiture pressure — one of the clearest cases in any sector of national security concerns overriding a completed transaction.

The sensitivity of this category reflects a distinctive feature of biological data: Unlike most commercial

information, genomic and patient-level data are irreversible strategic assets. Aggregated population-level genomic data can inform the development of precision diagnostics, targeted therapies, and — in the most extreme scenarios — precision biological weapons. U.S. regulations on bulk data transfers are partly a response to this vulnerability, though firms often find them cumbersome in the absence of a comprehensive national data privacy framework. The BIOSECURE Act, passed in 2024 and expanded in subsequent guidance, reinforces these concerns. It broadly defines "biotechnology equipment or services" to encompass sequencing technologies, bioinformatics tools, contract research services, and data-handling infrastructure — potentially affecting a wide range of relationships with Chinese-linked firms, including WuXi entities and BGI.

2. Life Sciences Services and Manufacturing Infrastructure

The second category comprises contract research organizations (CROs), contract development and manufacturing organizations (CDMOs), and bioanalytical services that form the backbone of drug development. This segment receives less attention in national security debates than genomics but may pose greater structural risk. A pattern of Chinese acquisitions has consolidated significant portions of preclinical testing, clinical trial execution, and active pharmaceutical ingredient (API) production under PRC-linked ownership: Tigermed's acquisition of Frontage Laboratories; WuXi PharmaTech's purchases of XenoBiotic Laboratories and Pharmapace; JOINN Laboratories' merger with Biomere; Pharmaron's acquisitions of Absorption Systems and a Rhode

61 Alice Zeng (Clarivate), quoted in "Is China the Future of Biotech?" *Labiatech*, December 13, 2024, <https://www.labiatech.eu/in-depth/china-biotech-industry/>. The figure of 89 new drug approvals refers to calendar year 2023 data compiled by China's National Medical Products Administration (NMPA)

Island API site formerly owned by Noramco; and the proposed, though ultimately blocked, Asymchem acquisition of Snapdragon Chemistry.

China's dominance in API production is a well-established vulnerability for the United States.

Ibuprofen, heparin, and numerous other widely used compounds depend on Chinese supply chains not only for finished APIs but also for key starting materials (KSMs), intermediates, and upstream excipients.

Efforts to friendshore API production to India have limited impact because India also depends on Chinese upstream inputs. The supply chain is therefore longer and more intertwined than headline API figures suggest. Strategic dependence cannot be addressed through API policy alone.

3. Therapeutic Pipeline Investment and New Company Structures

The third category involves venture financing for U.S. therapeutics companies and the growing use of U.S.-domiciled "new company" structures by Chinese biotech firms seeking access to the American market and regulatory pathways. Chinese firms such as Akeso have licensed drugs in development to U.S. firms, including Summit Therapeutics. This reverses the traditional direction of pharmaceutical licensing and reflects genuine advances in Chinese drug-development capability. China's advantages in the speed of R&D and clinical trials — products of both industrial policy and a regulatory environment that facilitates large-scale trials — make Chinese partnerships attractive to U.S. firms facing cost and timeline pressures.

At the same time, U.S. firms conducting significant human trials in China already transfer meaningful intellectual property and, in some cases, sensitive genomic data. The extent to which IP leakage already

occurs through established channels complicates the framing of Chinese investment as the primary vector of risk.

II. Sector-Specific Risks and Benefits

The life sciences sector presents an unusually acute version of the tension animating the Selective Openness framework. The industry is deeply collaborative by nature: Global drug development depends on cross-border research partnerships, clinical trial networks, and shared manufacturing infrastructure. At the same time, the sector generates some of the most sensitive data and strategic dependencies of any commercial industry. Restricting Chinese participation without equivalent capabilities elsewhere would impose real costs on U.S. innovation, while permitting participation without governance safeguards would create significant risks.

A. Benefits

- *Speed and scale in R&D and clinical trials.* Chinese clinical trial infrastructure offers U.S. firms significantly faster, lower-cost development timelines. As China becomes an essential market for commercially viable global drugs, a local trial presence also facilitates Chinese regulatory approval.
- *Manufacturing ecosystem and process know-how.* China's integrated pharmaceutical manufacturing ecosystem — spanning KSMs, intermediates, APIs, and finished dosage forms — offers efficiency advantages that U.S. firms cannot currently replicate domestically. Access to Chinese process know-how, not merely codified technology, could accelerate U.S. capability development in areas such as biologics manufacturing.
- *Pipeline access.* Chinese biotech firms have developed genuine therapeutic innovations that

U.S. firms want to license. A permissive licensing environment allows U.S. companies to access promising molecules without the governance complications of deeper investment structures.

- *Market dynamics.* China represents a major and growing pharmaceutical market. U.S. firms with Chinese investment partners may gain preferential access, while Chinese investors benefit from U.S. regulatory credibility and market scale.

B. Risks

- *Genomic and patient data.* The transfer of population-level genomic data is irreversible and strategically sensitive. Any investment structure that gives Chinese entities access to U.S. health data – directly or through affiliated data-handling infrastructure – requires the strictest governance controls.
- *IP leakage and process know-how transfer.* Minority investments and joint ventures create pathways for IP transfer that are difficult to monitor. The distinction between codified technology and tacit manufacturing expertise is critical: Licensing transfers the former, while joint ventures and foreign-owned subsidiary arrangements risk transferring the latter to Chinese partners.
- *Strategic supply chain dependencies.* Chinese investment that further embeds Chinese firms in API production and clinical trial infrastructure risks deepening rather than reducing existing dependencies. Governance frameworks for Chinese direct investment should be complemented by affirmative U.S. policies to build domestic and allied-country capacity.
- *BIOSECURE and regulatory uncertainty.* The broad scope of the BIOSECURE Act, combined with evolving regulations governing entities of

concern and federal procurement restrictions, creates significant uncertainty for U.S. firms navigating Chinese partnerships. Clear governance frameworks can reduce this uncertainty while maintaining meaningful oversight.

III. Applying the Three Investment Models to Life Sciences

The Selective Openness framework identifies three investment modes: licensing, joint ventures, and wholly foreign-owned subsidiaries. Each offers distinct benefits, limitations, and governance requirements. The life sciences sector is sufficiently heterogeneous that different modes are appropriate for different segments. The discussion below illustrates how each model maps onto the life sciences landscape and the degree of governance rigor each would require.

A. Licensing

Licensing is likely the most tractable for Chinese investment in U.S. therapeutic pipelines and, in limited circumstances, manufacturing process technology. It involves the lowest governance burden, the clearest contractual boundaries, and the least risk of operational entanglement. The Akeso-Summit Therapeutics arrangement illustrates this model: A Chinese firm with genuine innovation licenses a promising compound to a U.S. partner that retains full operational control over development and commercialization.

The primary governance concern in licensing is not control but dependence. Ongoing royalty arrangements, upgrade lock-in, and technology obsolescence can erode U.S. firms' operational autonomy over time. Licensing manufacturing process know-how poses a particular risk of transferring tacit knowledge through troubleshooting and technical

support relationships. Governance requirements for licensing arrangements should therefore focus on the following areas:

- Transparency requirements that disclose the licensor's relationships with PRC government entities and civil-military fusion activities.
- Technology domestication provisions requiring U.S. licensees to develop independent troubleshooting and process-modification capabilities within defined timelines.
- Restrictions, when necessary, on licensor personnel's access to U.S. facilities or data systems during technical support engagements.
- BIOSECURE Act compliance reviews to ensure that licensors are not covered entities under current or prospective regulatory definitions.
- Export control reviews of any process technology with potential dual-use applications.

The scale of the U.S. health care market gives American firms and regulators meaningful leverage to impose these conditions. Chinese biotech firms seeking access to U.S. patients, capital markets, and FDA credibility will generally accept reasonable governance requirements as the cost of entry. The precise mix of requirements can vary by investment.

B. Joint Ventures

Joint ventures (JVs) are well suited to the clinical trial and manufacturing infrastructure segments because the objective is capability building through co-investment and knowledge transfer rather than pipeline access alone. A U.S.-China JV involving a clinical research organization or biologics manufacturing facility could offer both parties genuine advantages: U.S. partners would gain access to Chinese efficiency and process know-how, while Chinese partners would gain access to U.S. regulatory

infrastructure, patient populations, and market credibility.

The governance risks of JVs in this segment are substantial. Codependent operations create deep integration that is difficult to unwind. Shared facilities and personnel create vectors for IP leakage and unauthorized data access. Asymmetric learning — in which Chinese partners systematically extract process know-how while U.S. partners remain dependent on Chinese personnel for critical functions — is a well-documented failure mode. Governance requirements for JVs should therefore be meaningfully stricter than those for licensing and should include tailored measures in the following areas:

- A U.S. National Security Compliance Committee with binding authority over data collection, personnel hiring for positions with systems access, IT architecture, and any cross-border information sharing. The committee should be staffed exclusively by U.S. persons with appropriate national security clearances.
- Complete physical and logical separation of U.S. systems and data from Chinese parent networks, with zero remote access from outside the United States.
- Technology-transfer milestones requiring periodic assessments of U.S. partner capability development. Ideally, the JV should produce genuine knowledge acquisition, not merely production access.
- Strict data-governance protocols that limit Chinese partner access to U.S. patient and genomic data, with real-time monitoring of cross-border data transmissions.
- A majority-independent U.S. board and a chief compliance officer who is a U.S. person and reports directly to the independent directors.

- CFIUS review based on pre-negotiated mitigation templates covering the measures above, reducing the cost and opacity of case-by-case negotiations.

C. Foreign-Owned Subsidiaries

Foreign-owned subsidiaries — Chinese-owned, U.S.-based operations — are most appropriate in the pharmaceutical manufacturing and medical equipment segments, where the primary benefits are capital investment, workforce development, and supply chain localization rather than access to data or intellectual property. United Imaging's establishment of small-scale U.S. manufacturing illustrates this model: A Chinese firm produces in the United States behind a tariff or regulatory wall, employs U.S. workers, and contributes to domestic production capacity.

Foreign-owned subsidiaries in life sciences raise the most complex governance challenges of the three models. Strategic decisions — including expansion, technology deployment, and supply chain relationships — remain with the foreign parent company. Knowledge spillovers are confined to individual workers rather than institutionalized within U.S. firms unless a robust local supplier ecosystem exists. Proximity to critical health infrastructure and sensitive patient populations further amplifies data and security concerns. Governance requirements should therefore be strictest for foreign subsidiaries in sensitive segments and should address the following areas:

- A strong presumption in favor of a full National Security Compliance Committee, with mandatory veto authority over all data-related, personnel, IT architecture, and partnership decisions.
- Supplier-diversification requirements mandating that foreign subsidiaries source from a diversified upstream supply base, including non-PRC suppliers, within defined timelines. Diversity, rather than total onshoring, should be the metric. Structured timelines and diversification targets can create predictability and stabilize market expectations.
- Local supplier-development requirements tied to government support, including tax credits and grants, to ensure that subsidiaries create demand for U.S. supplier networks rather than reproduce Chinese supply chains on U.S. soil.
- Facility-location restrictions prohibiting sites near sensitive government installations or critical health infrastructure.

IV. Complementary U.S. Policy Actions

The Selective Openness framework assumes that the United States has the capacity to absorb and benefit from Chinese investment. It presumes that domestic absorptive capacity, supplier ecosystems, and regulatory infrastructure are sufficient to capture knowledge spillovers rather than simply provide Chinese firms with U.S. market access and subsidies. In life sciences, this assumption is only partially warranted. Several complementary policy actions could make Chinese investment more productive and less risky.

A. Building Domestic API and Upstream Supply Capacity

The most important structural vulnerability in U.S. pharmaceutical supply chains is not Chinese ownership of U.S. assets but China's dominance in KSMs, intermediates, and auxiliary chemicals upstream of API production. A governance framework for Chinese direct investment must be paired with affirmative investment in domestic and allied-country

production of these inputs. Friendshoring to India offers limited near-term relief because India also depends on upstream inputs from China. Durable resilience requires investment in U.S. and allied-country chemical manufacturing capacity, supported through mechanisms analogous to the CHIPS Act in the semiconductor sector.

B. Establishing a National Genomic Data Governance Framework

The absence of a comprehensive U.S. data privacy law is an economic liability for the United States in life sciences. In its absence, the United States must rely on measures such as bulk-data-transfer regulations. A coherent national framework for genomic data governance — clarifying what data may be shared, under what conditions, and with what oversight — would reduce the compliance burden on U.S. firms and provide a clearer baseline for Chinese investment governance requirements. It would also bring U.S. practice into closer alignment with peer countries and reduce the asymmetry that disadvantages U.S. firms operating in China.

C. Leveraging Market Scale for Regulatory Reciprocity

The U.S. pharmaceutical market is large enough to set global terms. Chinese biotech and pharmaceutical firms seeking FDA approval, U.S. market access, and credibility in American capital markets may accept meaningful governance conditions in exchange. The United States could use this leverage explicitly by requiring, as a condition of market access or federal procurement eligibility, transparency about PRC government relationships, compliance with data-governance requirements, and participation in pharmaceutical-sector Information Sharing and

Analysis Centers (ISACs). This approach would extend the logic of the BIOSECURE Act while providing a more predictable and less discretionary framework than case-by-case exclusion. It may also offer advantages over a reciprocity-based approach, which would require broader consideration of the implications for U.S. trade and economic policy.

D. Clarifying the BIOSECURE Act's Scope and Transition Pathway

Uncertainty about the BIOSECURE Act's scope creates an unintended chilling effect on U.S.-China life sciences relationships. It deters partnerships that could be structured safely without necessarily preventing relationships that pose genuine risks. Clearer guidance on covered entities, permissible mitigation measures, and transition timelines would allow U.S. firms to make rational decisions about supply chains and partnership strategies. A mitigation pathway — analogous to CFIUS national security agreements — for covered entities willing to implement robust governance structures would extend the proposed framework into the BIOSECURE context. This parallels the broader recommendation that regulations governing foreign entities of concern must be more clearly defined for productive investment to materialize.

E. Holding Regular Consultation with Industry and Independent Experts

Assessing risks and remedies in the life sciences sector requires specialized knowledge of supply chains, research and development cycles, and advances in medicine and science. Industry experts told us that some U.S. government risk assessments have focused on far-fetched scenarios, such as precision bioweapons, while overlooking more immediate

risks. One example is the ongoing shortage of heparin, a drug used by a majority of U.S. hospital inpatients for procedures ranging from dialysis to open-heart surgery. Roughly 80 percent of the global heparin supply depends on pig intestines from China. The decimation of China's pig population by African swine fever, combined with escalating U.S.-China trade tensions, has left hospitals searching for alternatives with no reliable short-term solution. A regular, authoritative consultation mechanism could help assess supply chain dependencies and calibrate concerns about safety and resilience in life sciences.

F. Investment in Basic Research in Life Sciences

A thriving life sciences sector depends on a broader, healthy scientific research ecosystem. China's advances stem from increased funding for basic science as well as targeted industrial policies and market-making mechanisms. Innovation centers, including life sciences hubs, tend to emerge around major research universities, where dynamic basic research often finds commercial application. In Nature's 2026 global rankings of institutions by research output and influence, Harvard University is the only U.S. institution in the top 10; the others are Chinese universities and research centers. The strength of basic science research helps determine economic competitiveness and resilience in life sciences.

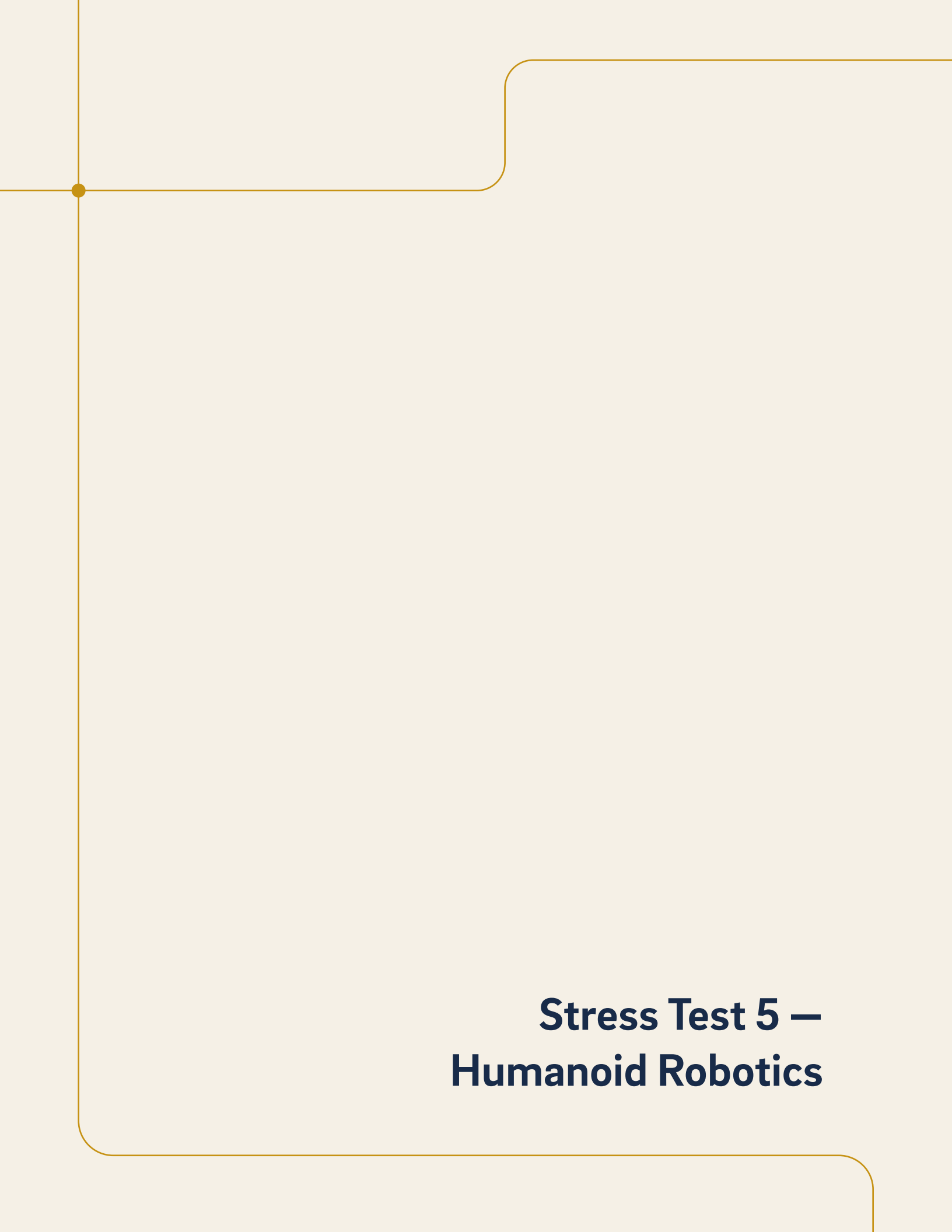
Conclusion

Life sciences is a particularly challenging sector in which to apply the Selective Openness framework because it combines unusually sensitive data assets, deep existing interdependencies, and genuine mutual interests. The required governance architecture — differentiated by investment mode, attentive to distinctions among data, IP, and manufacturing risks, and complemented by affirmative U.S. capacity building — is more demanding than in most other sectors. Yet the cost of error is correspondingly high in both directions: Exclusion forecloses real benefits and embeds existing dependencies without resolving them, while under-governed access creates risks to data, IP, and strategic supply chains that are difficult to reverse.

A sector-specific application of the framework, developed in consultation with industry and regulators, could provide the scaffolding for a principled and practical approach to Chinese investment in U.S. life sciences — one transparent enough to attract serious investors, rigorous enough to protect genuine national security interests, and flexible enough to accommodate the sector's inherent complexity.

More broadly, the life sciences sector demonstrates that Selective Openness requires differentiated governance rather than uniform restrictions. The risks associated with genomic databases, pharmaceutical manufacturing, contract research, venture investment and therapeutic innovation vary considerably and should be governed accordingly. A framework that distinguishes among these activities—while combining robust safeguards with complementary domestic investments—offers a more effective means of protecting national security while preserving the scientific collaboration, innovation and industrial capabilities that underpin long-term U.S. competitiveness.





Stress Test 5 – Humanoid Robotics

Stress Test 5 — Humanoid Robotics

Chinese Investment in the U.S. Humanoid Robotics Sector

By Paul Triolo, Center for China Analysis at Asia Society Policy Institute

Humanoid robotics sits at the intersection of advanced manufacturing, artificial intelligence and next-generation industrial systems, making it a particularly complex sector for foreign direct investment. As in clean energy and electric vehicles, Chinese firms have developed capabilities that the United States cannot easily replicate within a relevant time frame. Unlike those sectors, however, humanoid robotics adds another layer of complexity: the integration of sensor-rich hardware with continuously learning AI systems. This feature raises not only supply-chain and industrial-policy questions but also persistent concerns about data governance, system control and operational security.

The strategic question is not whether Chinese engagement will occur, but whether it can be structured to strengthen U.S. industrial capacity while containing risk. The broader framework, outlined in the Fair Terms for Safe Investment report, emphasizes that Selective Openness must be grounded in a clear assessment of economic benefits, national security risks and the capacity of U.S. firms and institutions to absorb and internalize foreign capabilities. In humanoid robotics, this balance is particularly delicate. The United States retains important advantages in frontier AI systems, high-performance computing and elements of the software stack. However, it lags significantly in the manufacturing ecosystems

required to scale complex electromechanical systems. China, by contrast, has built dense, vertically integrated supply chains and is extending those capabilities into robotics, supported by state-backed capital and an increasingly competitive domestic market.

Recent field observations by the author underscore both the scale and dynamism of China's humanoid robotics ecosystem. The sector remains early in its commercialization cycle, with firms experimenting across a wide range of use cases — from industrial automation and logistics to service and household applications — supported by a highly developed underlying supply chain. Dozens of robot original equipment manufacturers operate alongside a deep bench of component suppliers, reflecting a system-level capability that extends well beyond individual firms. As in the early days of electric vehicles, the ecosystem is characterized by rapid iteration, intense competition and strong pressure to move from prototype to production, even before end markets are fully mature.

Drawing on those observations, this stress test analyzes the strategic landscape of the humanoid robotics sector, the risks and benefits of Chinese direct investment, how three investment models might be applied, and complementary U.S. policy actions needed for success.

I. Strategic Landscape in Humanoid Robotics

China's position in humanoid robotics reflects a convergence of manufacturing scale, supply-chain integration and a dual-track innovation model spanning hardware and embodied AI. Much of the sector's early momentum derives from its overlap

with China's electric vehicle ecosystem, which provides a ready-made industrial base for key components such as batteries, sensors, actuators and control systems. This shared infrastructure has allowed Chinese firms to compress development timelines and push aggressively toward lower costs and greater manufacturability, replicating a pattern already observed in electric vehicles.

At the same time, the sector is evolving along two interdependent axes: the electromechanical "body" of the robot and the AI-driven "brain." Chinese firms have established clear advantages in the body layer, where cost, scale and integration dominate. Companies such as Unitree and UBTECH show how manufacturing density and supply-chain coordination translate into rapid product iteration and early deployment in industrial environments. Unitree's push toward lower-cost humanoids illustrates how quickly price-performance thresholds are shifting, while UBTECH's deployments in automotive factories highlight the sector's early convergence with existing industrial workflows.

In parallel, a more fragmented and competitive landscape is emerging around the "big brain" problem. Firms such as SenseTime and Tencent are developing embodied AI architectures that integrate perception, planning and control, while companies such as AgiBot and EngineAI are building data pipelines and simulation environments to support training and deployment. These efforts reflect a broader shift toward "model-of-models" architectures, in which language, vision and action systems are combined into hierarchical control frameworks. The resulting ecosystem is not yet consolidated, but it is already generating the data, tools and iterative cycles that will shape long-term competitive outcomes.

The United States, by contrast, has a more fragmented profile. Although U.S. firms remain at the frontier of AI model development, they lack the manufacturing ecosystems required to scale humanoid systems at comparable cost and speed. This asymmetry, common to many sectors examined in this report, is central to the Selective Openness framework: Chinese investment offers a pathway to manufacturing capability but may reinforce structural dependencies if it is not carefully managed.

II. Sector-Specific Risks and Benefits

A. Benefits

The potential benefits of structured engagement are substantial. Chinese firms bring manufacturing expertise, cost advantages and supply-chain coordination capabilities that could accelerate development of a U.S. robotics sector. As the broader framework notes, the alternative to structured engagement is not rapid domestic catch-up but a continued capability gap. Exposure to Chinese production systems could also catalyze local supplier networks and give U.S. workers access to advanced manufacturing techniques that are otherwise difficult to acquire.

B. Risks

The risks associated with Chinese investment in humanoid robotics extend beyond traditional foreign direct

investment concerns. As the broader framework emphasizes, the core policy challenge is to ensure that investment generates genuine capability formation rather than merely providing market access. In robotics, this challenge is particularly acute because value creation depends not only on components but also on the integration of hardware, software and data.

The most immediate concern is supply-chain dependence. Chinese firms dominate key segments of the humanoid “body stack,” including actuators, precision reducers, batteries, sensors and rare earth-based motor systems. These components are not easily substituted, and their production is embedded in supply chains that extend deep into China’s industrial base. Even leading U.S. efforts, such as Tesla’s Optimus program, remain dependent on Chinese suppliers for critical components, including rare earth magnets — a clear geopolitical chokepoint.

A second concern is the nature of technology transfer. As in clean energy, Chinese firms could replicate their production systems in the United States without transferring the underlying process know-how that drives competitive advantage. In robotics, this risk is amplified by the importance of tacit knowledge — calibration, integration and iterative refinement — that is difficult to codify or transfer through contractual arrangements alone.

The third and distinguishing concern is data governance. Humanoid robots operate as continuously learning systems that collect and process multimodal data from their environments. This includes visual and spatial information as well as data on human interactions and industrial processes. As Chinese firms increasingly rely on simulation, digital twins and world-model architectures, access to deployment data becomes a critical input into system improvement.

This creates a regulatory tension analogous to, but more complex than, the one posed by connected vehicles: Even when manufacturing is localized, data flows and control of software updates remain potential vectors of risk.

III. Applying the Three Investment Models

The Selective Openness framework emphasizes that the economic and security implications of foreign investment depend critically on the structure of that investment. In humanoid robotics, this insight is especially important because the sector is not a single value chain but a layered system: upstream components such as magnets, batteries, reducers, sensors and actuators; integrated robot “body” platforms; the “small brain” control systems governing locomotion and manipulation; and the “big brain” embodied AI layer connecting perception, planning, language and action. These layers present different learning opportunities and security risks. They therefore should not be governed by a single permissive or prohibitive rule. The appropriate policy question is not whether Chinese engagement in humanoid robotics is inherently acceptable or unacceptable, but which investment structures can generate genuine U.S. capability formation while mitigating supply-chain, data and control risks.

A. Licensing

Licensing arrangements offer the lowest-risk pathway for discrete technologies when the United States needs rapid capability acquisition but does not want Chinese firms to exercise operational control. In humanoid robotics, licensing could apply to battery systems, power electronics, perception hardware, certain servo drives and discrete manufacturing

processes for components such as sensors or end effectors. It may also be useful for parts of the “small brain” stack – motion-control software, simulation tools or manipulation modules – where U.S. firms could incorporate Chinese process know-how without granting the licensor access to U.S. deployment data.

This limitation is familiar from clean energy: Licensing can convey the “recipe” without the “cooking skills.” If a U.S. firm receives the right to use a component design or manufacturing process but not the tacit knowledge needed to troubleshoot, modify and improve it, the arrangement may deepen dependence rather than reduce it. This is a substantial risk in humanoid robotics because much of the value lies in calibration, integration and iterative refinement across the body stack.

The EngineAI example illustrates both the promise and the limits of this model. EngineAI appears to hold core intellectual property in joint design, motion-control systems and the data pipeline used to translate video and motion capture into robot-executable trajectories. The company also treats hands as modular, integrating third-party end effectors depending on the use case rather than insisting on full vertical integration.

That architecture suggests a possible licensing model for U.S. firms: acquiring access to specific motion-generation workflows, joint-control know-how or modular hand interfaces while keeping higher-risk deployment data, customer environments and model-training loops under U.S. control. To be worthwhile, such licensing would need domestication provisions, including access to process documentation and upgrade road maps; training for U.S. engineers; rights to modify software and hardware for U.S. deployment conditions; and a pathway to reduce dependence over time. The goal should not be simply to operate Chinese-designed robotics subsystems in the United

States, but to use them as a bridge toward U.S. process competence.

B. Joint Ventures

Joint ventures are more appropriate when learning depends on co-location, factory-floor problem-solving and integration of hardware with deployment workflows. In humanoid robotics, this includes actuator and joint manufacturing, integrated body platforms, dexterous manipulation systems, and industrial deployments in automotive, electronics, logistics and inspection settings.

UBTECH’s deployments in Chinese electric vehicle factories are instructive. The relevant capability is not merely the robot itself but the integration of humanoids into production environments, including task decomposition, line-side operations, uptime management and human-robot interaction. Similarly, AgiBot’s emphasis on data ecosystems and government-backed training sites points to the importance of co-located learning environments where robots generate task-specific data and improve through repeated deployment. A license may be insufficient in these areas because the transferable capability is embedded in the interaction among workers, robots, factory systems and iterative engineering teams.

For this reason, joint ventures would likely provide the greatest potential learning gains but also the greatest governance complexity. A robotics joint venture with a firm such as UBTECH, AgiBot, Fourier, Unitree or EngineAI could help U.S. partners learn how to scale integrated systems, manage component suppliers and adapt robots to real industrial settings. But the risks are equally clear: The Chinese partner could retain control over core technical functions; the U.S. partner could become an assembler rather than

a manufacturer; sensitive deployment data could flow back into Chinese training pipelines; and the venture could create a new dependence on Chinese components rather than a diversified U.S. supplier base.

Governance requirements would therefore need to be stricter than those for ordinary manufacturing joint ventures. They should include limits on foreign control, U.S.-controlled data environments, auditable software and update procedures, explicit technology-transfer milestones, workforce-training requirements, and supplier-diversification targets for components such as reducers, sensors, batteries and torque systems.

Emerging European Union policy frameworks provide a useful reference point. The European Commission's proposed Industrial Accelerator Act⁶² uses foreign investment policy not only as a security screen but also as an industrial-policy tool. For large investments in strategic manufacturing sectors, the proposal contemplates conditions such as foreign ownership caps, joint venture structures with EU participation, licensing of relevant intellectual property and know-how, research and development commitments, workforce requirements, and measures to strengthen EU value chains. The proposal seeks to ensure that foreign investment creates domestic value, employment and supplier development rather than merely providing market access to foreign firms.

Robotics is not currently among the core sectors highlighted in the EU proposal, which focuses on areas such as batteries, electric vehicles, solar energy and critical raw materials. But its logic maps well onto humanoid robotics: If foreign investment is allowed in

a strategic emerging sector, it should be conditioned on local capacity-building, not merely local sales or final assembly.

A U.S. version of this approach would not need to replicate the EU model mechanically, but it could borrow its core design principle: Approval should be tied to demonstrable domestic capability formation. A humanoid robotics joint venture should therefore be evaluated not only on ownership and security risk, but also on whether it builds U.S. engineering capacity, creates demand for local suppliers, trains workers and transfers process know-how. A venture that merely imports Chinese actuator modules, integrates them into robots in the United States and sends performance data back to China would fail the Selective Openness test. A venture that establishes U.S.-based actuator calibration, hires and trains U.S. engineers, sources some sensors and control electronics from U.S. or allied suppliers, and keeps deployment data under U.S. governance would be much more defensible.

C. Wholly Foreign-Owned Subsidiaries

Wholly foreign-owned enterprises, or WFOEs, present the most difficult case because they may scale quickly but generate weaker spillovers to U.S. firms. In humanoid robotics, a WFOE is most likely to take the form of final assembly, integration, service, maintenance, spare-parts or customer-support operations. Such a facility could be commercially attractive to firms seeking "Made in USA" signaling, proximity to customers, tariff mitigation and faster field support. It could also benefit U.S. workers by exposing them to advanced manufacturing and service

62 Jason Hewitt, Michael E. Leiter, and Wesley Lainé, "European Commission Proposes Industrial Accelerator Act: Prioritizing Strategic Sectors, 'Made in EU' Requirements and FDI Controls," Skadden, April 24, 2026, <https://www.skadden.com/insights/publications/2026/04/european-commission-proposes-industrial-accelerator-act>.

practices. The risk is that WFOEs reproduce Chinese supply chains on U.S. soil: Chinese-designed robots assembled from Chinese components and serviced by a local workforce, while strategic decisions, component sourcing, software architecture and product road maps remain controlled by the parent company in China.

The risk is particularly acute for firms whose advantages depend on vertically integrated access to China's component ecosystem. Unitree's cost-down momentum, for example, is closely tied to China-based sourcing and rapid manufacturing iteration. A U.S. Unitree-style facility might provide low-cost robots and service capacity, but without strong conditions it would not necessarily build U.S. competence in reducers, motors, sensors, batteries or integrated joints. The same logic applies to component-heavy firms in the Tesla Optimus supply chain. Chinese suppliers such as Sanhua, Tuopu, Green Harmonic, Shuanghuan and Keli/Coliy-type sensor firms may have real manufacturing value for U.S. robotics, but WFOE-style localization could simply shift final assembly without diversifying the underlying supply base.

Governance for WFOEs should therefore focus less on nominal localization and more on supplier diversification and structural separation. A robotics WFOE should be required to demonstrate phased sourcing from U.S. and allied suppliers where feasible, maintain auditable procurement and cybersecurity controls, and separate sensitive data functions from the foreign parent.

In lower-risk settings — education, research, entertainment or controlled commercial service deployments — these arrangements may be manageable. In higher-risk settings — critical infrastructure, defense-adjacent manufacturing,

hospitals, public safety or sensitive logistics — WFOEs should face much stricter constraints or be limited to hardware-service roles with U.S.-controlled software, data storage and model-update pathways.

The most sensitive layer is the "big brain." SenseTime's embodied-intelligence work and Tencent Robotics X's TAIROS platform show that Chinese firms are not simply producing robot bodies; they are building software architectures that fuse perception, planning, memory, locomotion, manipulation and cloud-mediated services. Tencent's TAIROS, for example, is positioned less as a single robot product than as a platform layer that could connect multiple robot manufacturers, developers and enterprise users. That architecture may be commercially attractive, but it raises sharper governance issues than a battery pack or actuator license. Licensing or joint venture access to big-brain software would require hard separation between U.S. deployment data and foreign model-training pipelines, restrictions on remote updates, third-party code review, and clear rules governing whether models may be retrained using U.S. sensor data.

D. Recommendations by Investment Type

The investment model should therefore vary by layer. Licensing is most appropriate for modular components and process know-how when U.S. firms can retain operational control. Joint ventures are most appropriate for integrated manufacturing and industrial deployment when learning requires co-location and shared engineering work. WFOEs may be acceptable for lower-risk assembly, service and support functions, but only when tied to local supplier development and strict data governance.

Big-brain software and embodied AI platforms require the highest level of scrutiny. They may need hybrid

structures that combine licensing, U.S.-controlled operating entities and continuous monitoring. This differentiated approach is the only way to avoid two undesirable alternatives: a blanket prohibition that slows U.S. learning or unstructured openness that gives Chinese firms access to the U.S. market while leaving the United States dependent on foreign-controlled robotics supply chains.

IV. What the Framework Requires to Work: Complementary U.S. Policy Actions

The success of Selective Openness in humanoid robotics will depend less on the formal structure of individual transactions than on the broader policy architecture governing how such systems are deployed, monitored and integrated into the U.S. economy. As the framework emphasizes, foreign investment cannot compensate for structural weaknesses in domestic capability. In robotics, those weaknesses are most visible in manufacturing ecosystems, supplier networks and the integration of hardware with data-driven software systems. Addressing these gaps requires sustained investment in advanced manufacturing infrastructure, workforce development and digital production systems. Without sufficient absorptive capacity, even well-structured Chinese investment — whether through licensing, joint ventures or subsidiaries — will generate limited spillovers and may reinforce dependence rather than build domestic capability.

At the same time, humanoid robotics poses governance challenges similar to those in life sciences because data are central to the technology. These systems are not static industrial goods but continuously learning, sensor-rich platforms that collect, process and transmit large volumes of multimodal data. This raises policy issues that the United States has only begun to address in adjacent domains such as social media and connected vehicles.

The experience with TikTok provides a useful, if imperfect, precedent. U.S. concerns about data access and algorithmic control led to efforts to impose structural separation, local data storage and third-party oversight through initiatives such as Project Texas. The process was protracted and politically contentious and ultimately led to an ownership restructuring that could provide a model⁶³ for some types of connected systems. The lesson for humanoid robotics is that data governance cannot be addressed after large-scale deployment. It must instead be embedded from the outset in investment conditions and regulatory frameworks through clear requirements for data localization, auditable software stacks, restrictions on remote access and enforceable mechanisms for ongoing monitoring.

Existing regulatory tools provide a starting point but will require adaptation. The Commerce Department's Connected Vehicle Rule⁶⁴ restricts the use of Chinese-origin information and communications technology and services components in vehicles because of risks of data exfiltration and remote manipulation. Its core logic — that sensor-rich, networked systems can serve

63 Daniel Castro, "Five Takeaways from the TikTok Deal," Information Technology and Innovation Foundation, January 26, 2026, <https://itif.org/publications/2026/01/26/five-takeaways-from-the-tiktok-deal/>.

64 U.S. Department of Commerce, Bureau of Industry and Security, "Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles," final rule, Federal Register 90, no. 10 (January 16, 2025): 5360, <https://www.federalregister.gov/d/2025-00592>.

as vectors for data collection and external control — maps directly onto humanoid robots. Humanoids, however, present a broader and more complex risk surface. Unlike vehicles, which operate within relatively defined environments and data regimes, humanoid robots may be deployed in factories, hospitals, homes and public spaces, where they interact directly with people and sensitive operational systems. Applying the Connected Vehicles Rule in its current form would likely be both overinclusive and underinclusive: It could restrict beneficial deployments in low-risk environments while failing to capture the full range of data and control risks associated with embodied AI systems. A modified framework would need to differentiate by use case and deployment context, incorporating tiered risk categories and corresponding governance requirements rather than a single blanket restriction.

Emerging legislative proposals⁶⁵ targeting humanoid robots — particularly those framed around banning federal procurement of Chinese-origin systems — reflect growing recognition of these risks. But they also risk repeating the limitations of a purely restrictive approach. As with earlier debates over Huawei and TikTok, blanket prohibitions may mitigate certain immediate security concerns but do little to address underlying capability gaps or shape the evolution of the technology ecosystem.

A more effective approach would integrate these concerns into the Selective Openness framework by establishing clear conditions under which investment and deployment are permissible. These could include requirements for structural separation of sensitive data functions, supplier diversification to avoid single

points of failure, and enforceable audit and compliance mechanisms. Rather than treating humanoid robotics as a binary “allow or ban” category, policy should define a spectrum of acceptable configurations tied to specific risk profiles.

Investment-screening mechanisms will also need to evolve. CFIUS remains effective at identifying and mitigating national security risks at the transaction level, but its mandate and processes are not well suited to evaluating the broader economic benefits of investment or managing the ongoing operational risks associated with data-intensive systems.

The TikTok case illustrates this gap. Even when risks can be conceptually mitigated through structural separation and governance arrangements, the absence of a clear, institutionalized framework creates prolonged uncertainty and politicization. Humanoid robotics requires a more integrated approach that combines transaction-level review with standardized governance templates, ongoing monitoring, and coordination among agencies responsible for data security, industrial policy and technology regulation.

Finally, credibility and predictability are essential for Selective Openness to function. As the broader framework underscores, Chinese firms and investors now operate in a global environment with multiple alternative markets and are less dependent on U.S. access than in previous decades. A fragmented and unpredictable regulatory environment — in which approvals may be reversed, conditions renegotiated or new restrictions imposed after the fact — will deter the forms of investment most likely to generate economic benefits. The experience of TikTok, along with uncertainty surrounding connected-vehicle

65 Humanoid Robotics Oversight and Blocking of Obtainment from Totalitarians Act of 2025 (Humanoid ROBOT Act of 2025), S. 3275, 119th Cong. (2025), <https://www.govinfo.gov/content/pkg/BILLS-119s3275is/html/BILLS-119s3275is.htm>.

and information and communications technology and services regulations, has already contributed to perceptions of regulatory risk. For humanoid robotics, clear and durable rules grounded in transparent principles and applied consistently will be critical to shaping investment flows rather than merely constraining them.

The policy challenge, then, is not simply to manage risk but to do so in a way that enables learning. Humanoid robotics remains an early-stage sector with uncertain use cases and rapidly evolving technological architectures. A rigid or overly precautionary framework could foreclose opportunities for the United States to participate in and shape that evolution. Conversely, a well-designed Selective Openness regime — combining targeted investment screening, robust data governance and complementary domestic investment — could allow the United States to capture the benefits of Chinese manufacturing and ecosystem strength while building its own long-term capabilities in what is likely to become a foundational technology domain.

NVIDIA's Jetson platform could become an important bridge technology in structured Chinese investment in U.S. humanoid robotics because it is already widely used by Chinese robotics firms for onboard perception, sensor fusion, motion planning and edge AI inference. In practice, Jetson gives Chinese robot developers a common, CUDA-adjacent edge-computing substrate that can support localization in the United States without immediately requiring a full redesign of a robot's control architecture.

This creates both an opportunity and a policy complication. On the positive side, a Jetson-based stack could make Chinese investment more technically legible to U.S. partners and regulators because the computing layer is supplied by a U.S. firm, supported

by a mature developer ecosystem and potentially auditable under U.S.-controlled software, data-storage and update rules. But it also underscores that humanoid robotics cannot be neatly separated into "Chinese hardware" and "American AI." Many Chinese firms are already building around U.S.-origin edge AI infrastructure.

Future controls on embodied AI computing could disrupt both Chinese robotics development and U.S. localization strategies. The Selective Openness framework should therefore treat Jetson-class systems as a potentially useful governance anchor — allowing Chinese robot bodies or components to be localized around U.S.-controlled edge computing, software auditability and data restrictions — rather than reflexively pushing the sector toward less transparent, non-U.S. alternatives.

Conclusion

Humanoid robotics presents a more complex and higher-stakes version of the challenge identified in clean energy. As in life sciences, the sector combines deep manufacturing dependencies with emerging data and control risks, accentuating the trade-offs inherent in Selective Openness. At the same time, the sector's early-stage development creates an opportunity to shape outcomes before competitive positions fully consolidate.

The central policy question is whether the United States can design an investment framework that captures the benefits of Chinese manufacturing capability while mitigating the associated risks. A differentiated approach — calibrated to investment structure, grounded in robust governance mechanisms and supported by complementary domestic policy — offers a plausible path forward. Without such a framework, the United States risks either slowing its

own progress through exclusion or reinforcing dependence through unstructured engagement.

Humanoid robotics illustrates why Selective Openness should be understood as a governance framework rather than a sector-specific policy. The appropriate approach depends not only on the technology involved, but also on the structure of investment, the source of economic value and the nature of the associated security risks. By distinguishing among investment models, technological layers and deployment contexts, policymakers can avoid the false choice between blanket exclusion and unstructured openness. Applied in this way, Selective Openness offers a durable framework for governing investment in strategic sectors while strengthening long-term U.S. technological and industrial capabilities under conditions of strategic competition.

Further References

- Paul Triolo, “A Deep (but Partial) Dive into China’s Humanoid Robotics and Embodied AI Sector,” AI Stack Decrypted (Substack), April 26, 2026, <https://pstaidecrypted.substack.com/p/a-deep-but-partial-dive-into-chinas>.
- Tencent Robotics X, TAIROS: Embodied AI Platform Overview (Shenzhen: Tencent, 2025), <https://robotics.tencent.com>.
- NVIDIA Corp., Jetson Platform for Robotics and Edge AI (Santa Clara, CA: NVIDIA, 2025), <https://developer.nvidia.com/embedded-computing>.
- Morgan Stanley Research, The Humanoid 100: Mapping the Humanoid Robot Value Chain (New York: Morgan Stanley, Feb. 6, 2025), https://advisor.morganstanley.com/john.howard/documents/field/j/jo/john-howard/The_Humanoid_100_-_Mapping_the_Humanoid_Robot_Value_Chain.pdf.
- Recorded Future, “The Future of Humanoid Robotics,” Insikt Group Research, Nov. 20, 2025, <https://www.recordedfuture.com/research/future-humanoid-robotics>.
- Mercator Institute for China Studies, Embodied AI: China’s Ambitious Path to Transform Its Robotics Industry (Berlin: MERICS, April 16, 2026), <https://merics.org/sites/default/files/2026-04/MER-RZ-Report-Embodied-AI-260422-Web.pdf>.
- U.S. Congress, Senate, American Security Robotics Act of 2026, S. 3275, 119th Cong., 1st sess., introduced March 26, 2026, <https://www.govinfo.gov/content/pkg/BILLS-119s3275is/html/BILLS-119s3275is.htm>.

china.ucsd.edu

UC San Diego

SCHOOL OF GLOBAL POLICY AND STRATEGY
21st Century China Center