LAW360

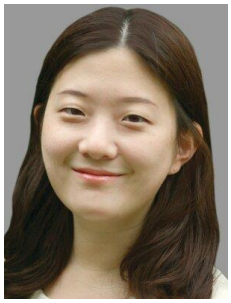
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Keeping Up With New US Push On Strategic Tech Competition

By **Stephenie Gosnell Handler, Chris Mullen and Claire Yi**
(September 19, 2022, 5:24 PM EDT)

Stephenie Gosnell Handler

Chris Mullen



Claire Yi

Recent actions by the U.S. government make clear that it views strategic competition surrounding emerging technologies as an urgent national security imperative.

This focus likely will only sharpen in coming months as the government increasingly explores novel legal and regulatory tools to supplement more traditional approaches to achieve national security objectives.

Key recent developments include:

- Legislative proposals to screen outbound investments;
- Funding restrictions designed to curtail expansion of semiconductor manufacturing abroad;
- White House consideration of using executive orders to protect technology competitiveness and restrict technology transfers; and
- The increasing use of export control restrictions.

Each of these developments is intended to enable the U.S. government to exert more control over outbound technology transfers, particularly aimed at curbing the potential flow of sensitive technologies or technologies of significant importance to U.S. national security to strategic competitors such as China and Russia.

While uncertainty remains over the precise mechanisms the government will leverage to achieve its national security objectives, it is increasingly clear that the government will supplement its traditional toolkit with innovative tools to do so.

Given this evolving landscape, companies should carefully consider their potential exposure and proactively assess their approaches to navigating geopolitical strategic competition.

Legislative Proposals for Outbound Investment Screening — Reverse CFIUS

The U.S. government's lack of visibility into outbound investments has recently gained heightened attention amid concerns that outbound capital flows and technology transfers could undermine national security objectives.

A new mechanism to implement outbound investment screening was introduced by Congress in the National Critical Capabilities Defense Act last year, and gained significant momentum this year.[1]

At its core, the NCCDA proposes to create a new interagency Committee on National Critical Capabilities that would function in a similar way to the Committee on Foreign Investment in the United States, or CFIUS, charged with reviewing inbound foreign investment.

The CNCC, however, would function in reverse and review outbound investment — hence its colloquial name "reverse CFIUS."

The list of outbound covered transactions that would be overseen by the CNCC broadly includes activities that could enhance a national critical capability of a country of concern or an entity of concern, in effect, giving significant interpretive power to the CNCC to define its mandate and to impose measures to mitigate perceived risks.[2]

Despite recent efforts over the summer months to modify the NCCDA for inclusion in other legislative packages, the proposed legislation is currently on the cutting room floor, with limited remaining opportunities to progress this year.

The current proposal has been met with significant criticism from the business community for its broad scope and significant authority.[3] However, the general concept of restricting certain types of outbound investment continues to garner bipartisan support that could lead to the establishment of outbound screening mechanisms in the future.

Guardrails on Offshoring of Semiconductor-Related Capacity

The CHIPS and Science Act, signed into law by President Joe Biden last month, did partially address underlying national security concerns regarding the offshoring of critical technological capabilities highlighted during pandemic-driven supply chain challenges.

Specifically, the CHIPS Act, while incentivizing investment in U.S. semiconductor manufacturing, also includes guardrails to prevent U.S. companies receiving subsidies under the act from engaging in significant transactions involving "the material expansion of semiconductor manufacturing capacity in the People's Republic of China or any other foreign country of concern."[4]

This legislation marks a historic departure for the U.S. government, which until recently had not significantly restricted private companies' strategies for offshoring and outsourcing technology outside traditional export control regimes.

While there exists some uncertainty as to what constitutes a significant transaction or a material expansion under the legislation, it is possible this act may lead to an overall chilling effect in the semiconductor industry for transactions involving China and other countries of concern.

Executive Push for Reviews on Inbound and Outbound Investment

In parallel with these legislative efforts, the White House's recent priorities have also included inbound and outbound investment restrictions to prevent technology transfers.

On Sept. 15, Biden signed a first-ever executive order defining the specific national security risk factors for CFIUS to consider in its inbound investment reviews.[5]

While the executive order does not change the CFIUS review process, it gives long-awaited and much-needed transparency into what may constitute core national security concerns, including:

- The security of critical U.S. supply chains;
- U.S. leadership in emerging technologies such as microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies; and
- Prevention of technology transfers in key U.S. industries.

The White House is also reportedly considering an executive order to establish its authority to review outbound technology investment.[6] The precise contours of the executive order appear to be under discussion and may depend on the outcome of further legislative discussions.

Yet, public sources generally forecast that the executive order could require disclosures for any investments in Chinese advanced technologies and establish a system, similar to the CNCC, that could block investments to China and potentially other countries of concern.[7]

Earlier this year, National Security Adviser Jake Sullivan provided some indication of the government's likely approach, stating that "it is important to have the ability to limit narrow classes of investments that raise national security concerns, using rulemaking that would engage a broad variety of stakeholders."[8] Given this appetite, an executive order, if issued, may be narrower in scope than the proposed NCCDA.

Export Controls for Microchips and Semiconductors

Controlling the manufacture and supply of microchips and semiconductors lies at the heart of the strategic competition policy discussions surrounding emerging technologies. In recent weeks, the U.S. government has deployed both traditional and nontraditional methods to strengthen control over these strategic supply chains and to limit the export of these key technologies to strategic competitors, most notably China and Russia.

Consistent with its traditional authorities, on Aug. 12, the U.S. Department of Commerce's Bureau of Industry and Security, or BIS, issued an interim rule to implement new controls on four Section 1758 technologies[9] — named after the section of the Export Control Reform Act of 2018 that tasked the department with regulating emerging and foundational technologies.[10]

These measures impose new restrictions on certain ultrawide band gap semiconductors and certain emerging electronic computer aided design software in a clear effort to limit the ability of U.S. adversaries to produce advanced technologies for their militaries.[11]

While these new additions to the commerce control list demonstrate the department is actively exercising traditional authorities to control emerging technologies, the slow pace of defining and implementing controls underscores the limitations of the U.S. government relying solely on the department's traditional authorities, particularly given the speed of innovation and the broader geopolitical landscape.

In response, the department has demonstrated increased willingness to employ more novel authorities as well. In an unusual move, in late August, the department appears to have leveraged a relatively obscure provision of the Military End Use/User Rule that permits BIS to, without any formal rulemaking process, privately inform parties that a license is required for specific exports of any item due to an "unacceptable risk of use in or diversion to a 'military end use' or a 'military end user.'"[12]

In this case, BIS appears to have utilized this mechanism to impose additional restrictions on Nvidia Corp.'s export to China, including Hong Kong, and Russia of certain advanced integrated circuits and associated technology used in sophisticated artificial intelligence applications, as revealed in the company's U.S. Securities and Exchange Commission Form 8-K disclosure.[13]

Soon after, the U.S. government appeared to backtrack somewhat on these restrictions according to an updated filing on Sept. 1, in which the company noted it had received certain time-limited authorizations to continue to service U.S. customers, fulfill orders through the company's Hong Kong facility, and to engage in export activities necessary to develop certain chips.[14]

This temporary reprieve was likely designed to address the unintended global supply chain disruptions caused by the government's initial mandate — including that some of the targeted processors appear to have been developed in the company's Hong Kong facility.

Nvidia's tribulations are not unique — news reports indicate Advanced Micro Devices Inc. was also notified of a separate licensing requirement for the export of certain processors to China and Russia.[15]

These novel efforts to more closely control strategic supply chains may very well be a harbinger of broader restrictions to come, including greater use of the nonpublic notification provisions of the MEU Rule.

These situations similarly underscore the difficulty of effectively using existing export control mechanisms amidst globalized supply chains — often with complex and geographically distributed development, sourcing, and manufacturing facilities — as such actions carry the potential for unintended business interruptions and compliance challenges.

What Is Next and How Can You Be Prepared?

While the legal and regulatory tools on the horizon may be novel, the policy areas of focus, namely U.S. technology and military competitiveness, are longstanding areas of U.S. interest with broad bipartisan support. The Biden administration and U.S. Congress have both made clear they will continue to view technology transfers and investments in strategic competitors with greater scrutiny and will leverage a broad government approach to curb the activities deemed the greatest threat to U.S. national security.

In this rapidly evolving landscape, companies should review potential areas of exposure and potential mitigation strategies, including the following:

- Carefully trace and document tracing of supply chains from cradle-to-grave to understand potential weaknesses and areas of exposure, and consider potential alternatives.

- Ensure proper export controls and sanctions compliance measures are in place to manage the flow of goods and technology across borders, including at the local business unit level.

- Review current and future mergers, acquisitions, and investments for potential areas of heightened concern with regard to ownership, board membership, and technologies involved.

- Ensure proper operating procedures are in place to prevent unauthorized technology transfers both within the United States and abroad.

- Proactively develop response strategies for emerging technologies that could be designated as Section 1758 technologies and subject to enhanced restrictions in the near future, potentially with little warning.

As the geopolitical landscape continues to fracture, companies will need to remain vigilant of shifts in the regulatory landscape and be prepared to respond quickly to such changes in order to mitigate business impacts, including potentially significant losses to revenue.

Stephenie Gosnell Handler is a partner, and Chris R. Mullen and Claire Yi are associates, at Gibson Dunn & Crutcher LLP.

[1] See National Critical Capabilities Defense Act of 2021, H.R. 6329, 117th Cong. (2021); National Critical Capabilities Defense Act of 2021, S. 1854, 117th Cong. (2021).

[2] National Critical Capabilities Defense Act of 2021, H.R. 6329, 117th Cong. (2021).

[3] See, e.g., Letter from Advanced Med. Tech. Ass'n et al. to Members of the U.S. Congress (June 22, 2022), https://www.uschamber.com/assets/documents/220623_Coalition_NationalCriticalCapabilitiesDefenseAct_Congress_2022-06-24-125102_nlcb.pdf.

[4] Supreme Court Security Funding Act of 2022, Pub. L. No. 117-167, § 103 (2022).

[5] Press Release, White House, FACT SHEET: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States (Sep. 15, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/fact-sheet-president-biden-signs-executive-order-to-ensure-robust-reviews-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states/.

[6] See, e.g., Jennifer Jacobs & Daniel Flatley, Biden Weighing Actions to Curb US Investment in China Tech, Bloomberg (Sept. 2, 2022), https://www.bloomberg.com/news/articles/2022-09-03/biden-weighing-actions-to-curb-us-investment-in-china-tech?leadSource=uverify%20wall; John D. McKinnon,

White House Weighs Order to Screen U.S. Investment in Tech in China, Other Countries, Wall St. J. (Sept. 8, 2022), https://www.wsj.com/articles/white-house-weighs-order-to-screen-u-s-investment-in-tech-in-china-other-countries-11662674581.

[7] The anticipated executive order is reportedly part of a broader policy toward China in development. Public sources have stated that the Biden Administration is also considering a separate executive order that would control Chinese internet companies' collection of data on U.S. citizens, as well as another that would restrict the types of technology that can be sold to China. See Reed Albergotti, Semafor Exclusive: Biden Will Crack Down on Chinese Tech with a New Executive Order (Sept. 2, 2022), https://medium.com/semafor-media/semafor-exclusive-biden-will-crack-down-on-chinese-tech-with-a-new-executive-order-da466c263a8a. These executive orders, if issued, would mark a significant policy development. As discussed in our 2021 Year-End Sanctions and Export Controls Update, in June 2021, President Biden revoked three Trump-era executive orders targeting TikTok and other applications developed by Chinese companies, after significant legal challenges were brought against them, and instead ordered the Commerce Department to investigate the national security risks of "connected software applications." See Gibson, Dunn & Crutcher LLP, 2021 Year-End Sanctions and Export Controls Update (Feb. 4, 2022), https://www.gibsondunn.com/2021-year-end-sanctions-and-export-controls-update. In light of this, future actions specifically targeting Chinese internet companies will likely require additional effort from the U.S. Government to preempt future legal challenges.

[8] Ellen Nakashima, White House Wants Transparency on American Investment in China, Wash. Post (July 13, 2022), https://www.washingtonpost.com/national-security/2022/07/13/china-investment-transparency.

[9] In a May 23, 2022 rule, BIS stated that it would no longer distinguish between so-called "emerging" and "foundational" technologies as stipulated in Section 1758 of the Export Control Reform Act of 2018. Instead, these technologies are now collectively referred to as "Section 1758 technologies." Commerce Control List: Controls on Certain Marine Toxins, 87 Fed. Reg. 31,195, 31,196 (May 23, 2022).

[10] Implementation of Certain 2021 Wassenaar Arrangement Decisions on Four Section 1758 Technologies, 87 Fed. Reg. 49,979 (Aug. 15, 2022). While the majority of these controls went into effect on August 15, 2022, certain controls associated with new ECCN 3D006 do not go into effect until October 14, 2022. Notably, the interim rule enacts recent decisions by the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, a group composed of 42 governments around the world charged with developing multilateral export controls.

[11] Id.

[12] 15 C.F.R. § 744.21(b).

[13] NVIDIA Corporation, Form 8-K (Aug. 31, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001045810/000104581022000146/nvda-20220826.htm.

[14] NVIDIA Corporation, Form 8-K (Sept. 1, 2022), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001045810/000104581022000151/nvda-20220831.htm.

[15] Don Clark & Amanda Swanson, U.S. Restricts Sales of Sophisticated Chips to China and Russia, N.Y. Times (Aug. 31, 2022), https://www.nytimes.com/2022/08/31/technology/gpu-chips-china-russia.html.