WILMERHALE

Executive Order Raises Regulatory Risks for Foreign Investment Across U.S. Economy

SEPTEMBER 19, 2022

On September 15, 2022, President Biden signed an Executive Order (EO) identifying economic sectors that merit special attention for review by the Committee on Foreign Investment in the United States (CFIUS or the Committee). While the EO does not change CFIUS's jurisdiction to review foreign investments in US businesses, it marks the first time a US president has singled out particular factors that the Committee should use when evaluating whether a transaction presents a threat to US national security. The EO will likely have the effect of expanding the number of foreign investments CFIUS reviews. It specifically directs CFIUS to undertake national security risk assessments with an eye toward the impact a transaction may have on supply chain security, US technology leadership, cybersecurity, access to sensitive personal data, and the impact of incremental investments over time.

The EO reinforces a practical reality that has become increasingly clear over the past several years: foreign investments into large swaths of the US economy may generate attention from CFIUS. CFIUS is likely to focus in particular on investments by foreign entities in technologies perceived as important to US strategic leadership, such as semiconductors and microelectronics, quantum computing, batteries, autonomous vehicles, robotics, and artificial intelligence. And the EO makes clear that companies that may not think of themselves as important to US strategic national security can nevertheless attract CFIUS's notice, including companies in biotechnology and biomanufacturing, advanced clean energy, climate adaptation, critical materials, and agriculture sectors.

This EO lands amid a bipartisan focus on the national security concerns that can be triggered by foreign direct investment. In August, CFIUS reported to Congress that the Committee is reviewing a record number of transactions for national security risk, and the Biden administration and Congress are considering either an executive order or legislation to screen outbound US investment in semiconductors and similar technologies through a "reverse CFIUS" process.

The administration "will continue to examine whether additional steps are necessary to best posture CFIUS to protect US investors from predatory foreign investments," National Security

Advisor Jake Sullivan said after the EO was released.

EO Summary: Sharpening CFIUS Focus

The EO directs CFIUS to consider five sets of factors when conducting their reviews:

1. Supply Chains. CFIUS is to consider a transaction's effect on "supply chain resilience and security, both within and outside the defense industrial base." The defense industrial base refers to the businesses that the US Department of Defense relies upon to provide military equipment. The EO highlights a wide swath of civilian industrial supply chains that CFIUS should consider, including "microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements)," and elements of the agriculture sector. The Committee is to consider how a transaction might make the United States vulnerable to supply chain disruptions. CFIUS should also consider several factors involved in the supply chain itself, including its diversification through alternative suppliers, including allies and partners; whether the US government itself relies on the supply chain; and the concentration of ownership or control over the supply chain by a foreign party.

The EO warns of the risks of foreign investments that shift the control of critical supply chains to a foreign party, including to a foreign party that has "relevant third-party ties" "that might cause the transaction to pose a threat to national security." The emphasis on "third-party ties," a phrase that is not further defined but is repeated throughout the EO, suggests the Committee will be on the lookout for links between the foreign investor and other foreign parties. While the EO names no nations of particular concern, the administration is acutely concerned about competitors like China and Russia, and CFIUS will probably scour transactions for links to entities of those countries.

2. Technological Leadership. The EO directs the Committee to consider a transaction's effect on US technological leadership. It enumerates specific areas of concern, including critical minerals, "microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies." CFIUS is to consider relevant ties by the foreign buyer and its investors or other third parties "that might cause the transaction to threaten to impair the national security of the United States."

3. Investment Trends. CFIUS shall consider incremental investment trends in a technology sector that, in aggregate, "may cede, part-by-part, domestic development or control in that sector or technology" to a foreign person. "[A] series of transactions over time can increase systemic vulnerability, potentially resulting in a particular covered transaction giving rise to national security risk," a senior administration official explained during a background press call, suggesting CFIUS should look beyond the specific factors of the transaction before it when assessing the national security risks to broader industry trends.

4. Cybersecurity Risks. The EO directs CFIUS to consider the cybersecurity capabilities of the foreign investor and cybersecurity practices of the domestic target. In particular, the Committee should review whether a transaction could provide a foreign party "with the capability and intent to conduct cyber intrusions or other malicious cyber-enabled activity." Such activities include those

attempting to affect the outcome of elections, the operation of US critical infrastructure and the integrity of US communications. CFIUS is also to consider the cybersecurity posture and practices of all parties to the transaction that could allow a foreign party to conduct such cyber activities. The EO notes that Congress, in the Foreign Investment Risk Review Modernization Act of 2018, which broadened CFIUS's mandate and passed with near-unanimous support, identified "exacerbating or creating new cybersecurity vulnerabilities" as a relevant consideration for CFIUS.

5. Sensitive Data. The EO directs CFIUS to consider sensitive data in several ways. First, CFIUS is to consider whether a covered transaction involves a US business that has *access* to US persons' sensitive data, "including United States persons' health, digital identity, or other biological data and any data that could be identifiable or de-anonymized, that could be exploited to distinguish or trace an individual's identity in a manner that threatens national security." Second, seemingly out of counterintelligence concerns, CFIUS is to consider whether the target company has access to data on "sub-populations" that a foreign entity could use to target individuals or groups "in a manner that threatens national security." Third, CFIUS is to consider whether a transaction involves the *transfer* of US persons' sensitive data to a foreign entity "who might take actions that threaten to impair the national security of the United States," including whether the foreign entity has ties to investors that may exploit the information, including through commercial means.

The EO directs the Committee to review its practices on an ongoing basis and "to continue to make any updates as needed and appropriate to ensure that the Committee's consideration of national security risks remains robust alongside changes to the national security landscape." CFIUS is to provide periodic reports to the White House, including any policy recommendations.

Contributors

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

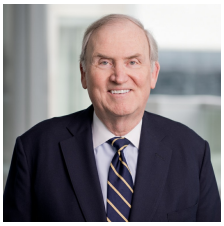
+1 202 663 6195

Matthew F. Ferraro

COUNSEL

matthew.ferraro@wilmerhale.com

+1 202 663 6562



Ambassador Robert M. Kimmitt

SENIOR INTERNATIONAL COUNSEL

Co-Chair, Crisis Management and Strategic Response Group

robert.kimmitt@wilmerhale.com

+1 202 663 6250

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770