LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins CFIUS & US National Security Practice September 26, 2022 | Number 3012

New CFIUS Executive Order Outlines 5 Risk Factors: Key Takeaways

President Biden sends a message to foreign investors and the business community that CFIUS will closely scrutinize transactions presenting certain risk factors.

On September 15, 2022, President Biden issued an Executive Order (the EO) relating to national security reviews conducted by the Committee on Foreign Investment in the United States (CFIUS). This is the first Executive Order since CFIUS was established in 1975 that provides "direction" to CFIUS to ensure that CFIUS reviews "remain[] responsive to evolving national security risk." While the EO does not expand CFIUS' jurisdiction or the process by which CFIUS conducts its reviews, the EO provides sharpened guidance to CFIUS on five risk factors that CFIUS must consider as it reviews a proposed transaction's potential impact on US national security. As noted in a White House statement released at the same time, the EO also "acknowledges the importance of continuous improvements to the foreign investment review process and directs CFIUS to continue to regularly review its processes, practices, and regulations to ensure that they remain responsive to evolving national security threats."

The 5 Risk Factors

The EO articulates five risk factors associated with a proposed transaction: 1) supply chain resilience, 2) US technological leadership, 3) aggregate investment trends, 4) cybersecurity, and 5) US persons' sensitive data.

Two of the factors (cybersecurity and US persons' sensitive data) elaborate on existing national security factors identified in the CFIUS governing statute (Section 721 of the Defense Production Act of 1950, codified at 50 USC 4565(f)). The remaining factors are not expressly mentioned in the CFIUS statute or implementing regulations, but are nevertheless unsurprising, as these risk factors officially describe trends that CFIUS has been increasingly scrutinizing over recent years.

1. Supply chain resilience: The EO instructs CFIUS to consider a proposed transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base. The EO notes that foreign investments in certain key sectors may undermine supply chain resilience efforts and render the United States vulnerable to future supply disruptions.

When considering a transaction's potential effect on supply chain resilience, CFIUS must consider the following elements in particular:

- the degree of the foreign person's involvement in the US supply chain, including but not limited to the concentration of ownership or control;
- the United States' capability with respect to manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security;
- the degree of diversification through alternative suppliers across the supply chain; and
- whether the US business supplies, directly or indirectly, to the US government, the energy sector industrial base, or the defense industrial base.

2. US technological leadership: The EO also instructs CFIUS to consider a proposed transaction's effect on US technological leadership in sectors important to US national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, and elements of the agricultural industrial base that have implications for food security.

To protect US technological leadership in these sectors, CFIUS is to consider whether a transaction can reasonably be expected to result in future advancements and applications in technology that could undermine national security. The EO also provides that the Office of Science and Technology Policy (OSTP), in consultation with other CFIUS members, will periodically publish a list of technology sectors the OSTP assesses to be fundamental to US technological leadership in areas relevant to national security.

3. Aggregate investment trends: The EO directs CFIUS to consider aggregate industry investment trends or the series of transactions related to the single transaction before the Committee. The EO underscores the risks incremental investments over time can pose in a sector or technology, as such investments may cede domestic development or control or facilitate harmful technology transfer to a foreign person.

4. Cybersecurity: The EO directs CFIUS to consider whether a transaction can provide a foreign person with direct or indirect access to capabilities that heighten the risk of malicious cyber-enabled activities (such as breaching databases housing sensitive data, interfering with elections in the United States, or sabotaging critical energy infrastructure such as smart grids). The EO directs CFIUS to consider the cyber security posture, practice, capabilities, and access of both the foreign person and the US business.

5. US persons' sensitive data: The EO directs CFIUS to consider the risks posed by a foreign person's access to sensitive data of US persons. The EO recognizes data as a powerful tool for surveillance, tracing, tracking, and targeting individuals, and acknowledges that advances in technology allow re-identification or de-anonymization of formerly unidentifiable data.

Specific factors for CFIUS to consider include:

- whether the US business has access to US persons' sensitive data (including health, digital identity, or other biological data and any data that could be identifiable or de-anonymized);

- whether the US business has access to data on sub-populations in the US that could be used by a foreign person to target individuals or groups of individuals;

- whether a transaction involves the transfer of US persons' sensitive data to a foreign person; and

- whether the foreign person has ties with relevant third parties that have the ability to exploit such data or that have sought to exploit such information.

Key Takeaways

By identifying these five risk factors, the President has memorialized trends that have been increasingly clear over recent years, as CFIUS has taken a broad view of factors that raise a proposed transaction's national security concerns.

- **Looking beyond the transaction under review:** The EO expressly encourages CFIUS to focus beyond a specific proposed transaction before it. The EO instructs CFIUS to consider not only the threat posed by a foreign person that is party to a notified transaction, but to also consider the risks presented by the foreign person's commercial, investment, non-economic, and other relevant third-party ties. CFIUS will also evaluate the possibility of future advancements and application in technology that could undermine national security as a result of the proposed transaction, not only the US business' present technologies. The EO also signals that CFIUS will review a transaction not only on a case-by-case basis, but also with respect to systemic threats, challenges, and patterns. To this end, CFIUS must consider whether a foreign person has made investments in or acquisitions in the same, similar, or related sectors in the past.

- **Specific industry sectors of interest:** The EO identifies specific sectors that present a heightened risk to US technological leadership and/or supply chain resilience and security. These sectors are microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, climate adaptation technologies, and elements of the agricultural industrial base that have implications for food security. Many of these sectors have recently been subject to enhanced scrutiny by the US government through other channels. For example, according to recent reports, several of these sectors are possible areas of focus of a potential "reverse" CFIUS regime that would create review of certain outbound investment or similar activities from the United States into certain foreign countries. (For more on a possible "reverse" CFIUS, see Ready for a "Reverse" CFIUS? Four Takeaways From New Bipartisan Bill.)

- **Reemphasizing concern about personal data:** Reiterating one of the key areas of focus of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), the EO confirms that CFIUS will continue to closely scrutinize transactions involving US businesses with access to personal data of US persons. Notably, the EO does not limit the Committee's focus to what the FIRRMA defines as "sensitive personal data," but takes a broader focus on all sensitive data of US persons.

The EO is an important expression of many areas of focus for CFIUS' national security reviews. The EO provides the President's imprimatur on CFIUS' consideration of a broad set of factors when assessing potential national security concerns associated with a proposed transaction. This affirms CFIUS' historically broad discretion to determine national security risks.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

James H. Barker
james.barker@lw.com
+1.202.637.2200
Washington, D.C.

Les P. Carnegie
les.carnegie@lw.com
+1.202.637.1096
Washington, D.C.

Damara L. Chambers
damara.chambers@lw.com
+1.202.637.2300
Washington, D.C.

Ruchi G. Gill
ruchi.gill@lw.com
+1.202.654.7126
Washington, D.C.

Asia Cadet
asia.cadet@lw.com
+1.202.637.2251
Washington, D.C.

Julie Choi Shin
juliechoi.shin@lw.com
+1.202.637.1003
Washington, D.C.

Matthew J. Crawford
matthew.crawford@lw.com
+1.617.880.4588
Washington, D.C.

Zachary N. Eddington
zachary.eddington@lw.com
+1.202.637.2105
Washington, D.C.

Allison K. Hugi
allison.hugi@lw.com
+1.202.637.1088
Washington, D.C.
