KIRKLAND & ELLIS

Kirkland Alert

President Biden Issues First-Ever Directive to CFIUS on National Security Considerations in Transactions

21 September 2022

On September 15, 2022, President Biden issued an Executive Order (the "EO") regarding the Committee on Foreign Investment in the United States ("CFIUS" or "the Committee") and its evaluation of national security risks associated with inbound foreign investment. While the EO does not alter CFIUS's legal jurisdiction or the timelines for CFIUS reviews, it offers new and important clarifications for transaction parties and CFIUS member agencies and signals to market participants what types of transactions may raise national security concerns. Notably, the EO is the first Presidential directive specifically addressing the risk factors that CFIUS should consider when reviewing a transaction within its legal jurisdiction (a "covered transaction") since CFIUS's establishment in 1975.

CFIUS's implementing statute identifies a variety of factors for CFIUS to consider when reviewing covered transactions and evaluating the potential effects of such transactions on U.S. national security, including a transaction's potential effects on "domestic production needed for projected national defense requirements [and] United States international technological leadership in areas affecting United States national security." CFIUS may also consider "other factors as the President or the Committee may determine to be appropriate."

The EO explicitly instructs CFIUS to consider five national security factors in its reviews, the first two of which — supply chain security and technological leadership — supplement existing factors identified in the statute, and the latter three of which — investment trends, cybersecurity and sensitive data — identify "additional factors" not identified in the statute for CFIUS to consider in reviewing deals. We summarize these factors below, and provide related takeaways.

1. The EO directs CFIUS to consider a transaction's impact on the **security and resilience of critical supply chains**, including those that may fall outside of the traditional U.S. defense industrial base. CFIUS should consider, for example, the security and resilience of supply chains relating to manufacturing, artificial intelligence, critical mineral and material resources, advanced clean energy and climate adaptation technologies, microelectronics and other key sectors that were identified last year in a separate executive order that addressed supply chain issues.[1]
2. The EO instructs CFIUS to consider a transaction's **potential harm to U.S. technological leadership** in key areas impacting U.S. national security, including by assessing whether a transaction may in the future lead to technological developments that could undermine U.S. national security. Relatedly, the EO instructs a CFIUS member, the White House's Office of Science Technology and Policy, to periodically publish a list of technology sectors that it "*assesses are fundamental to United States technological leadership in areas relevant to national security.*"
3. The EO also indicates that CFIUS should consider the **cumulative effects of multiple transactions** involving the same, or related, parties within the same sector or involving similar technologies (particularly in certain sensitive sectors or technologies), even where the particular transaction under review may not give rise to national security concerns when considered by itself.
4. The EO directs CFIUS to consider **potential cybersecurity risks** arising from a transaction and, in particular, whether the transaction would permit a foreign investor to gain access to sensitive cybersecurity infrastructure such as elements of election infrastructure or energy infrastructure (e.g., smart grids).
5. The EO instructs CFIUS to assess a transaction's impacts on potential **commercial or other "access" to, and use or transfer of, sensitive data of U.S. persons** (e.g., biometrics or "digital identity") by foreign parties (either directly involved in the transaction or through third-party relationships) that may exploit the information in a manner that "*threatens national security.*"

Takeaways

- **The EO is an important "signaling" mechanism to market participants regarding the national security policy priorities that CFIUS will consider in its reviews.** The EO provides helpful guidance to transaction parties in conducting due diligence for transactions that may require or warrant a CFIUS filing. For example, investors with "*relevant third party ties*" (i.e., independent relationships with vendors, limited partners, or other third-parties involving persons or countries of concern

that could indirectly pose a threat to U.S. national security if the underlying transaction occurs) should assess how these "third party" risks may affect how CFIUS evaluates a particular transaction. This is particularly true where the transaction otherwise implicates a sector or technology identified in the EO (e.g., artificial intelligence or quantum computing). Likewise, with respect to sensitive data, the EO specifies that even access through commercial interactions is relevant to CFIUS's national security considerations.

- **The EO highlights CFIUS's increasing attention to the cumulative threat posed by a pattern of investment by a specific foreign investor.** This approach follows on CFIUS's description of threats posed by "multiple acquisitions" in its recently published annual report.[2] Given the historical understanding that CFIUS's reviews were conducted on a transaction-by-transaction basis, it is significant that the EO instructs CFIUS to take a broader view, thus confirming an ongoing trend by the Committee of viewing transactions in a wider investment context.
- **The EO does not change CFIUS's legal jurisdiction or the process of CFIUS reviews.** CFIUS timelines remain the same, and CFIUS will continue to assess national security risk of both voluntarily notified and non-notified transactions as a function of (i) the "threat" of the foreign investor, (ii) the "vulnerability" of the U.S. business, and (iii) the "consequence" of the interaction between the threat and vulnerability. Rather than initiating a paradigm shift, the EO memorializes factors that have become increasingly more relevant to CFIUS reviews in practice, but that have not been consistently described in formal or public ways.
- **CFIUS is, and will continue to be, a significant actor in broader U.S. national security and industrial policy — but it is not the sole actor.** Transaction parties should assess the potential implications of coincident U.S. executive, legislative and regulatory actions, including (as may be relevant) the passage of the recent *CHIPS and Science Act*, which President Biden signed into law on August 26, 2022, as well as expected future regulations including those related to export controls for emerging and foundational technologies and outbound investment reviews.

---

1. https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ ↩

2. As described further in a prior Kirkland *Alert* covering seven highlights from CFIUS' Latest Annual Report ↩

Authors

Chad B. Crowell

Associate / Washington, D.C.

Daniel J. Gerkin

Partner / Washington, D.C.

Lucille Hague

Partner / Washington, D.C.

Erika Krum

Associate / Washington, D.C.

Mario Mancuso, P.C.

Partner / Washington, D.C. / New York

William G. Phalen

Partner / Boston

Ivan A. Schlager, P.C.

Partner / Washington, D.C.

Related Services

Practices

- International Trade & National Security

Suggested Reading

- 06 November 2024 Kirkland Alert Bureau of Industry and Security Proposes Rulemaking Impacting Importation and Sale of Hardware and Software for Connected Vehicles with a Nexus to China and Russia
- 26 April 2024 Kirkland Alert CFIUS in its Enforcement Era

- 05 March 2024 Kirkland Alert An Unacceptable Risk: Groundbreaking Executive Order Restricts Outbound Transfers of U.S. Personal Data and Government-Related Data to Countries of Concern