wiley

ALERT

New Executive Order Directs CFIUS to Consider Additional National Security Factors in Evaluating Covered Transactions

September 19, 2022

On September 15, 2022, President Biden signed an executive order (EO) that reaffirms longstanding U.S. open investment policy and elaborates and expands on the existing list of statutory factors that the Committee on Foreign Investment in the United States (CFIUS or the Committee) may consider when reviewing transactions to assess their potential impact on U.S. national security.

The EO does not change existing CFIUS processes or legal jurisdiction, but rather elaborates on two existing national security factors and defines three additional factors for the Committee to consider when reviewing covered transactions. While CFIUS is not limited in the factors it may consider during the course of its review and has historically considered many if not all of the factors outlined in the EO, the administration has stated that the EO will guide the Committee and "help businesses and investors better identify early on national security risks arising from transactions to help them determine whether to file with CFIUS."

The EO provides additional direction to CFIUS with respect to two existing national security factors described in Section 721(f)(3) and (f)(5) of CFIUS's authorizing statute:

> ***1. Supply chain resiliency.*** The EO directs the Committee to consider a covered transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base, in manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security, including microelectronics, artificial

Authors

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Daniel P. Brooks
Partner
202.719.4183
dbrooks@wiley.law

Paul J. Coyle
Associate
202.719.3446
pcoyle@wiley.law

Practice Areas

Committee on Foreign Investment in the United States (CFIUS)

Cybersecurity

International Trade

National Security

Strategic Competition & Supply Chain

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), elements of the agriculture industrial base that have implications for food security, and any other sectors identified in section 3(b) or section 4(a) of Executive Order 14017 of February 24, 2021 (America's Supply Chains).

Relevant considerations include the degree of diversification through alternative suppliers, including suppliers located in allied or partner economies; supply relationships with the U.S. government and/or relevant industrial bases; and concentration of ownership or control by the foreign person in a given supply chain.

2. U.S. technological leadership. The EO directs the Committee to consider whether a covered transaction involves manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to United States technological leadership, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies.

The EO also directs CFIUS to consider whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine national security. To inform the Committee's decisionmaking in this regard, the EO requires the White House Office of Science and Technology Policy (OSTP) to periodically publish a list of technology sectors assessed to be fundamental to U.S. technological leadership in areas relevant to national security.

The EO also directs the Committee to consider the following additional factors that are not currently included in CFIUS's authorizing statute:

3. Aggregate industry investment trends. The EO notes that "[i]ncremental investments over time in a sector or technology may cede, part-by-part, domestic development or control in that sector or technology" and that certain investments could therefore pose a limited threat when viewed in isolation but may be concerning when considered in the context of previous transactions. Such transactions may facilitate harmful technology transfer in key industries or otherwise harm national security through the cumulative effect of these investments. Accordingly, the EO directs CFIUS to consider the risks arising from covered transactions in the context of multiple acquisitions or investments in a single sector or in related manufacturing capabilities, services, critical mineral resources, or technologies.

To inform the Committee's decisionmaking in this regard, CFIUS may request as part of its review that the Commerce Department's International Trade Administration provide the Committee with an analysis of the industry or industries in which the U.S. business operates, and the cumulative control of, or pattern of recent transactions by, a foreign person in that sector or industry.

4. Cybersecurity. The EO directs the Committee to consider whether a covered transaction may provide a foreign person with direct or indirect access to capabilities or information databases and systems on which threat actors could engage in malicious cyber-enabled activities affecting the interests of the

United States or U.S. persons, including activity designed to undermine the protection or integrity of data in storage or databases or systems housing sensitive data; activity designed to interfere with U.S. elections, critical infrastructure, the defense industrial base, or other cybersecurity national security priorities; or the sabotage of critical energy infrastructure, including smart grids.

The EO also directs the Committee to consider the cybersecurity posture, practices, capabilities, and access of the foreign person and the U.S. business that could allow a foreign person to manifest cyber intrusion and other malicious cyber-enabled activity within the United States.

5. Sensitive data. The EO directs the Committee to consider whether a covered transaction involves a U.S. business that (i) has access to or that stores U.S. persons' sensitive data, including 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, or (ii) has access to data on sub-populations in the United States that could be used by a foreign person to target individuals or groups of individuals in the United States in a manner that threatens national security. The EO also directs the Committee to consider whether a covered transaction involves the transfer of U.S. persons' sensitive data to a foreign person.

With respect to each of the five factors described above, the EO directs CFIUS to consider not only the risk profile of the foreign person involved in the transaction but also whether the foreign person has commercial, investment, non-economic, or other ties (relevant third-party ties) with other foreign persons, including foreign governments, that might cause the transaction to pose a threat to U.S. national security.

In addition to elaborating and expanding on the national security factors that CFIUS may consider when reviewing transactions to assess their potential impact on U.S. national security, the EO acknowledges the importance of continuous evaluation and improvement to the foreign investment review process. Accordingly, the EO directs CFIUS to regularly review its processes, practices, and regulations to ensure they are responsive to evolving national security threats and to implement any updates as needed.

Wiley has an unparalleled ability to assist clients with investments that raise national security concerns. Our team has direct experience within the government managing the CFIUS process and assisting clients on CFIUS reviews. We have more than two decades of experience handling matters involving national security, including CFIUS, Team Telecom, the Defense Counterintelligence and Security Agency, U.S. sanctions and export control laws, and supply chain security, and have counseled clients in transactions that involve nearly every industry sector subject to CFIUS review.

Please reach out to any of the authors listed on this alert should you have any questions about the EO or the CFIUS regulations governing foreign investment.

Jack Wroldsen, a Trade Analytics Coordinator at Wiley Rein LLP, contributed to this alert.