Executive Order Outlines Expansive National Security Considerations for CFIUS

September 21, 2022

Key Points

- EO 14083 provides updated guidance to CFIUS regarding its consideration of U.S. national security risk factors and is aimed at confronting evolving and emerging threats to U.S. technological leadership, U.S. supply chain resilience, cybersecurity and the sensitive personal data of U.S. citizens.
- While the EO does not modify CFIUS's existing legal jurisdiction or regulatory processes and does not significantly alter the way that CFIUS has been assessing national security risks in recent years, it does provide a helpful roadmap for parties seeking to understand what CFIUS considers to be a national security concern in the current environment. Along those lines, this order may be helpful for parties assessing whether a voluntary filing may be appropriate for a transaction where national security risks may not be readily apparent.
- Notably, the EO underscores that transactions involving foreign investors from allied and partner countries may present risks due to such investors' "third-party ties" (e.g., commercial, supply chain, non-economic) to other foreign parties from "foreign adversaries" or "countries of special concern."

Background

The Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") is the inter-agency mechanism through which the U.S. government formally monitors and reviews foreign investment in the United States for possible national security concerns. CFIUS has the authority to initiate reviews of transactions, suspend transactions, impose mitigation measures and recommend that the President block pending transactions or order divestitures of completed transactions when national security concerns cannot be mitigated. Parties can voluntarily file with CFIUS to obtain clearance to address the risk that CFIUS will intervene in a pending or completed transaction. In certain cases, filing with CFIUS is mandatory.

On September 15, 2022, President Biden issued Executive Order 14083 ("EO"), "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," that provides formal presidential direction

Contact Information

If you have any questions concerning this alert, please contact:

Christian C. Davis
Partner
chdavis@akingump.com
Washington, D.C.
+1 202.887.4529

Katherine P. Padgett
Counsel
kpadgett@akingump.com
Washington, D.C.
+1 202.887.4079

John A. Gurtunca
Associate
jgurtunca@akingump.com
Washington, D.C.
+1 202.887.4122

Thor Petersen
Associate
tpetersen@akingump.com
Washington, D.C.
+1 202.887.4307

to CFIUS on factors the Committee must consider when determining the effects of a transaction on U.S. national security. Significantly, this is the first time the U.S. government has issued official national security guidance related to foreign direct investment since 2008.

A primary objective of the EO is to help guide the Committee's standard assessment of the national security risks presented by a covered transaction, including by pointing to specific emerging and evolving threats that CFIUS should consider when assessing the threat posed by the foreign investor, the vulnerability of the U.S. business and potential consequences to U.S. national security that could result from the exploitation of those vulnerabilities by a threat actor.

New National Security Risk Factors

Resilience and Security of Supply Chains

The EO's focus on supply chain resilience is premised on the notion that foreign investment can make supply chains more vulnerable to future supply disruptions by shifting ownership, rights or control with respect to certain manufacturing capabilities, services, critical mineral resources or technologies to a foreign investor with the means and intent to impair U.S. national security. To account for such risk, the EO directs CFIUS to assess the transaction's impact on the resilience and security of supply chains related to the following sectors:

1. microelectronics
2. artificial intelligence
3. biotechnology and biomanufacturing
4. quantum computing
5. advanced clean energy (such as battery storage and hydrogen)
6. climate adaptation technologies
7. critical materials (such as lithium and rare earth elements)
8. elements of the agriculture industrial base.

Whether a particular transaction involving one of the above sectors poses a risk to U.S. national security will depend on facts such as (i) the foreign person's degree of involvement in the relevant supply chain; (ii) U.S. capability with respect to the relevant manufacturing capabilities, services, critical mineral resources or technologies at issue; (iii) degree of diversification through alternative suppliers across the supply chain (including suppliers located in partner and allied countries); (iv) whether the U.S. business that is the target of the transaction supplies, directly or indirectly, the U.S. government, the energy sector industrial base or the defense industry base and (v) the concentration of ownership and control by the foreign investor in the given supply chain.

U.S. Technological Leadership

The EO directs CFIUS to consider the transaction's impact on U.S. technological leadership, specifically the manufacturing capabilities, services, critical mineral resources or technologies related to:

1. microelectronics
2. artificial intelligence
3. biotechnology and biomanufacturing
4. quantum computing
5. advanced clean energy
6. climate adaptation technologies.

The EO's direction to consider whether the transaction could result in "future advancements and applications" of a particular technology demonstrates that parties should not limit their considerations to merely the current commercial use of a particular product, but also whether it has any potential military applications, for example. The EO also instructs the White House Office of Science and Technology Policy to periodically update the above list with additional technology sectors that are considered "fundamental" to U.S. technological leadership.

Aggregate Industry Investment Trends

The EO also directs CFIUS to consider whether the transaction is part of a series of acquisitions or investments in a single sector, based on the potential for incremental acquisitions to result in gradually ceding domestic development or control in that sector or technology over time in a way that may not be apparent from just a transaction-specific inquiry. The EO identifies the facilitation of technology transfer in key industries as one harmful effect of such cumulative transactions. To assist with its consideration of this potential risk factor, CFIUS may request the International Trade Administration to provide an analysis of the industry or industries in which the target U.S. business operates, and the cumulative control of, or pattern of recent transactions by, a foreign person in that sector or industry.

Enhancing Malicious Cyber Capabilities

In addition, the EO instructs CFIUS to consider whether a transaction would enable malicious cyber activities that could (i) undermine the protection or integrity of data in storage or in databases or systems housing sensitive data; (ii) interfere with U.S. elections, critical infrastructure or the defense industrial base; or (iii) sabotage critical energy infrastructure, including smart grids. With respect to specific transactions, relevant facts include the cybersecurity capabilities of the foreign investor and the cybersecurity practices of the target U.S. business.

Sensitive Personal Data

Finally, building on the recent focus that CFIUS has given to transactions involving access to the sensitive personal data of U.S. citizens, the EO directs CFIUS to consider whether the transaction affords a foreign investor access to sensitive data, in particular health and biological data. A transaction will present heightened risks regarding sensitive personal data where the U.S. business at issue (i) has access to U.S. persons' sensitive data, including U.S. persons' health, digital identity or other biological data or any data that could be identifiable or de-anonymized, which could be "exploited to distinguish or trace individuals' identities" or (ii) has access to data on "sub-populations in the United States" that could be used to "target individuals or groups of individuals." The EO's emphasis on advances in technology, combined with

access to large data sets that enable the “re-identification” or “de-anonymization” of previously unidentifiable data, demonstrates that disaggregated or anonymized data sets will no longer be a silver bullet to avoiding CFIUS scrutiny.

Third Party Ties

In assessing the threat presented by a foreign investor in a transaction, the EO instructs CFIUS to consider the foreign investor’s “relevant third-party ties” to other foreign persons and foreign governments as part of the Committee’s standard threat analysis of the foreign investor. As a result, even transactions involving foreign investors from partner and allied countries may be associated with a higher threat profile based on any commercial (e.g., customers and suppliers), investment (e.g., minority investors) and non-economic relationships (e.g., familial and political ties) to other foreign persons from “foreign adversaries” or “countries of special concern” that may not be apparent from the face of an investor’s formal ownership and control structure.

Conclusion

While the EO largely memorializes CFIUS's current practice with respect to assessing national security considerations in transactions, the EO does highlight a few points that are particularly noteworthy. These include the emphasis on (i) the foreign investor’s third-party ties to foreign adversaries or countries of special concern; (ii) whether the transaction will afford the foreign investor access to large sets of (even anonymized) sensitive data; and (iii) whether the transaction involves a sector identified as “fundamental” to U.S. technological leadership –microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy and climate adaptation technologies. Along those lines, the EO provides a helpful roadmap for parties, particularly with respect to weighing the pros and cons of making a voluntary filing.

akingump.com