PUBLICATION

New CFIUS Executive Order Clarifies Review Factors for Evolving National Security Landscape

Authors: Prentiss Lee Smith, Aldo M. Leiva
September 20, 2022

On September 15, 2022, President Biden signed an Executive Order (EO) adding five additional factors for The Committee on Foreign Investment in the United States (CFIUS) to consider when reviewing transactions. The identified factors focus on transactions that may appear to be an economic transaction undertaken for commercial purposes but present an unacceptable risk to U.S. national security. The EO, however, does not include an anticipated outbound investment screening mechanism.

The EO builds on the Administration's prior executive orders, which raise concerns about investment and espionage from China and supply chain vulnerabilities.[1, 2] CFIUS is often seen as a "black box" and this EO is intended to give businesses greater clarity.

The EO directs CFIUS to consider five specific sets of factors:

1. A given transaction's effect on the resilience of critical U.S. supply chains that may have national security implications, including those outside of the defense industrial base
2. A given transaction's effect on U.S. technological leadership in areas affecting U.S. national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies
3. Industry investment trends that may have consequences for a given transaction's impact on U.S. national security
4. Cybersecurity risks that threaten to impair national security
5. Risks to U.S. persons' sensitive data

The EO furthers the goals of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) to make CFIUS more responsive to emerging national security risks. Following FIRRMA's implementation, CFIUS reviewed a record number of covered transactions in 2021, including 272 notices, 164 declarations, and 130 investigations.[3] More information about FIRRMA can be found here.

Analysis of the Five Factors

6. **Critical U.S. Supply Chain Resiliency.** The EO specifies that CFIUS should examine the impact of a transaction on supply chains, including those outside the defense industrial base. The EO identifies concerns with transactions shifting ownership, rights, or control of critical minerals, manufacturing capabilities, and services.

7. **Effect on U.S. Technology Leadership.** Supply chains may be considered "vulnerable" if they are not sufficiently diversified through alternative suppliers, not located in the US or an allied nation, or ownership is concentrated. Notably, the EO mentions that CFIUS should consider "non-economic or other ties (relevant third-party ties)" when determining risks posed by a transaction.

The EO specifies industries that CFIUS should focus on that underpin U.S. technological leadership in areas affecting national security. It identifies the following industries as technologies that are critical to national security:

- 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)
- Elements of the agriculture industrial base that have implications for food security
- Other technologies are expected to be identified in the future by the White House Office of Science and Technology Policy

8. **Industry Investment Trends and U.S. National Security.** Other technology sectors are expected to be identified in the future. The EO instructs CFIUS to examine trends, particularly with an eye towards technology transfer, within a given sector. Going forward, CFIUS will consider not only the significance of a transaction in insolation, but risk in the context of "multiple acquisitions or investments" in a sector.

9. **Cybersecurity Risks.** The EO also requires a careful assessment of cybersecurity and privacy risks within the context of the observed strategy of foreign adversaries to obtain access to sensitive data and technologies. Transactions that involve investments by foreign persons with both the capability and intent to conduct cyber intrusions, cyberattacks, and other malicious activity shall require an assessment on whether such foreign persons (or related third-parties) may have access to conduct such activities. In addition, the cybersecurity posture, practices, capabilities, and access of all parties to the transaction shall also be considered as part of any CFIUS analysis.

10. **U.S. Persons' Sensitive Data.** Similarly, as to privacy risks, transactions that allow access to large data sets of U.S. persons' sensitive data are subject to focused review, given the heightened capabilities of foreign adversaries using advanced technology to de-anonymize what was once unidentifiable personal data. The EO clarifies that such transactions shall include an assessment of whether the foreign investor has, or parties to whom the foreign investor has ties, have sought or have the ability to exploit such personal data to the detriment of national security, whether by commercial or other means. Taken together, these factors should be read in conjunction with the national security factors already set forth in the CFIUS statute, with the understanding that the factors are intended to be illustrative, and that CFIUS may consider any national security risk arising out any transaction within its jurisdiction.

Transactional parties should consider the following practical steps in addressing these cybersecurity and privacy concerns:

11. Analyze policies and procedures of all involved parties, and interview security officials to fully understand and validate how cybersecurity controls operate in practice
12. Compare and align technical and administrative safeguards with such global cybersecurity standards as ISO 27001 and/or NIST 800-171/171a
13. Perform a comprehensive review of data assets, with identification of controlled/regulated data types, such as controlled unclassified information (CUI) or International Traffic in Arms Regulations (ITAR) data

14. Consider migration of regulated data to a highly secure environment
15. Confirm that critical/export-controlled technology, intellectual property, and trade secrets are appropriately protected
16. Implement additional monitoring and auditing capabilities in place for CFIUS-related reporting regarding these five factors

If you have any questions about CFIUS compliance, please contact P. Lee Smith, Aldo M. Leiva, or any member of Baker Donelson's International Trade and National Security practice.

[1] Executive Order 14034, Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries June 09, 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/

[2] Executive Order 14017, Executive Order on America's Supply Chains, February 24, 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[3] CFIUS Public Annual Report to Congress CY 2021: https://home.treasury.gov/system/files/206/CFIUS-Public-AnnualReporttoCongressCY2021.pdf