THOMPSON HINE

International Trade Update

October 2022

Biden Issues Executive Order to Focus the Consideration of National Security Factors in the CFIUS Review Process

Key Notes:

- The Executive Order does not change the review process or legal jurisdiction of CFIUS.
- The Executive Order revised the national security factors for CFIUS to include in its foreign investment review process.
- OSTP shall publish a list of technology sectors fundamental to U.S. technology leadership and national security.

On September 15, 2022, President Biden issued Executive Order (E.O.) 14083 to elaborate upon existing statutory factors and include additional national security factors the Committee on Foreign Investment in the United States (CFIUS or "Committee") must consider in its review process of a covered transaction. This marks the first time a president has issued a formal presidential directive on CFIUS-related matters since President Carter's E.O. in 1975 which established the Committee. The E.O. does not change the Committee's review process or legal jurisdiction, but it must be considered in conjunction with the national security factors already set out in the CFIUS' authorizing statute (*see* Section 721 of the Defense Production Act of 1950, as amended). "The United States welcomes and supports foreign investment," the Order begins. "Some investments in the United States by foreign persons, however, present risks to the national security of the United States, and it is for this reason that the United States maintains a robust foreign investment review process focused on identifying and addressing such risks."

Ensuring U.S. Supply Chain Resiliency

The E.O. elaborates upon several of the existing national security statutory factors CFIUS considers in its review of a covered transaction. Specifically, the E.O. mandates CFIUS to consider the foreign investment's "effect on supply chain resilience and security, both within and outside of the defense industrial base," as well as how the foreign investment will impact U.S. technological leadership, especially in manufacturing capabilities services, critical mineral resources, and technologies. CFIUS should consider "the degree of involvement" by a foreign person who is a party to the covered transaction to minimize dependency on that foreign person. Consequently, CFIUS must analyze not only the concentration of ownership or control the foreign person has in a given supply chain, but also whether the covered transaction may undermine the resilience and security of supply chains that are critical to national security. In fact, to further safeguard national security, the Order mandates the Committee to consider a foreign person's third-party ties to other foreign persons or foreign governments to reduce the risk of a third-party beneficiary using the transaction to threaten or impair the national security of the United States.

Protecting U.S. Technological Leadership

The Order charges CFIUS to evaluate the covered transaction's effect on U.S. technological leadership in key sectors where national security could be threatened including, but not limited to, microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum

ATTORNEY ADVERTISING

computing, advanced clean energy (such as battery storage and hydrogen), climate adaptation technologies, critical materials (such as lithium and rare earth elements) and elements of the agriculture industrial base that have implications for food security. The E.O. also addresses whether the foreign person in a covered transaction has relevant third-party ties that might cause the transaction to pose a threat, and whether a covered transaction “could reasonably result in future advancements and applications in technology” that have the potential to undermine national security. To assist CFIUS in identifying technology sectors of concern, the E.O. directs the Office of Science and Technology Policy (within the Executive Office of the President) to periodically publish a list of technology sectors it deems as fundamental to U.S. technological leadership in areas critical to national security.

Incremental Investment Risks

The Order directs CFIUS to consider any “incremental investments” made over time by the foreign person in the same, similar or related U.S. sectors or industries as the covered transaction. As noted by the Order, a cumulative review of investment trends not only allows CFIUS to contextualize the individual transaction considering the aggregate, but also enables the Committee to analyze the gradual ownership or control by a foreign person of critical infrastructure, assets, resources or technologies within key industries. Assessing a foreign person’s historical investments will also permit CFIUS to consider the national security implications if such transactions involve possibly harmful technology transfers. To assist CFIUS in tracking multiple investments by a foreign person, the E.O. empowers the International Trade Administration within the Department of Commerce to help review “the cumulative control of, or pattern of recent transactions by, a foreign person, including directly or indirectly, a foreign government, in that sector or industry.”

Assessing Cybersecurity Risks

The E.O. requires CFIUS to consider any cybersecurity risks, such as cyber intrusions or the introduction of malicious cyber-enabled activity, posed by a covered transaction. For example, CFIUS must factor whether a foreign investment will “exacerbat[e] or creat[e] new cybersecurity vulnerabilities,” including cyberactivity designed to affect the outcome of any election, the operation of critical U.S. infrastructure like smart grids, the defense industrial base or the confidentiality, integrity or availability of U.S. communications. Similarly, the Order tasks CFIUS to identify and assess how information databases and systems, especially those housing sensitive data, will directly or indirectly be threatened by the covered transaction. Finally, CFIUS must consider the cybersecurity posture, practices, capabilities and access of the foreign person, or their relevant third-party ties, who might take actions or conduct cyber intrusion activities that could threaten or impair the national security of the United States.

Safeguarding Sensitive Information and Personal Data

In acknowledging increasing national security concerns surrounding personal data and recognizing data as an increasingly powerful tool for surveillance, tracing, tracking and targeting of individuals or groups of individuals, the E.O. mandates CFIUS to consider whether a covered transaction involves a U.S. business retaining large data sets that may “expose, directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that [sensitive] information in a manner that threatens national security.” The Order requires CFIUS to identify U.S. businesses that will be involved in the covered transaction and to consider the risks posed by any foreign investment or control, especially if a U.S. business (1) has access to the health, digital identity or other biological data of a U.S. person or sub-population of individuals, or (2) possesses sensitive data that can identify or be de-anonymized to distinguish a U.S. person or sub-population of individuals for subsequent exploitive, tracing or targeting purposes. The E.O. also directs CFIUS to consider whether the foreign investor, or relevant third-party ties, have sought to or can exploit such information to the detriment of national security, including through commercial or other means.

OSTP to Identify Fundamental Technology Sectors

The Office of Science and Technology Policy ("OSTP") within the White House has been tasked under the E.O. with periodically publishing a list of technology sectors that it assesses are fundamental to U.S. technological leadership in areas relevant to national security. The member agencies of CFIUS are directed to consider these technologies, as appropriate, when conducting any national security review.

Next Steps for Foreign Investors Making Investments in the United States

The E.O. introduces new challenges for foreign businesses and investors preparing to invest in the United States. The Order expands the list of national security factors, articulates the precise meaning of each factor and obliges CFIUS to incorporate this refurbished and more robust list of factors in its review process. Although the E.O. does not dramatically change the focus of U.S. national security considerations, it is likely to lead to additional questions and requests for information during the CFIUS review process.

Thus, foreign entities contemplating an investment in the United States should seek legal advice pertaining to any transaction to identify national security concerns early in the transaction process. This is of particular importance for foreign persons who intend to invest in sectors or industries within U.S. supply chains that have consequences for U.S. national security, or for foreign persons that are repeat investors seeking to procure greater market share within sectors or industries in U.S. supply chains that have consequences for U.S. national security.

FOR MORE INFORMATION

For more information, please contact:

Francesca M.S. Guerrero
Partner, International Trade
202.973.2774
Francesca.Guerrero@ThompsonHine.com

Samir D. Varma
Partner, International Trade
202.263.4136
Samir.Varma@ThompsonHine.com

Scott E. Diamond*
Senior Legislative & Regulatory Policy Advisor, International Trade
202.263.4197
Scott.Diamond@ThompsonHine.com
**Not licensed to practice law*

Aaron C. Mandelbaum*
Law Clerk, International Trade
202.973.2737
Aaron.Mandelbaum@ThompsonHine.com
**Not admitted to the practice of law*

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2022 THOMPSON HINE LLP. ALL RIGHTS RESERVED.