King & Spalding
Client Alert

SEPTEMBER 19, 2022

For more information, contact:

Stephen J. Orava
+1 202 661 7937
sorava@kslaw.com

Christine E. Savage
+1 202 626 5541
csavage@kslaw.com

J. Philip Ludvigson
+1 202 626 9267
pludvigson@kslaw.com

Alexis J. Early
+1 202 626 9622
aearly@kslaw.com

Jamieson L. Greer
+1 202 626 5509
jgreer@kslaw.com

Adam Harper
+1 202 393 3799
arharper@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Suite 900
Washington, D.C. 20006
Tel: +1 202 737 0500

Executive Order Directs CFIUS to Consider National Security Factors

Ensuring a responsive CFIUS in an evolving national security landscape

On September 15, 2022, President Biden signed an Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (the "Order") that explicitly ties the role, actions, and capabilities of the Committee on Foreign Investment in the United States ("CFIUS") to the Administration's overall national security priorities, including enhancing U.S. supply chain resilience, preserving U.S. technological leadership, ensuring robust cybersecurity, and protecting Americans' sensitive data.

CFIUS is an interagency committee authorized to review transactions involving foreign investment in the United States and real estate transactions by foreign persons to determine the effect of such transactions on U.S. national security. Notably, the Order is the first since CFIUS was created nearly five decades ago that provides formal Presidential direction on national security factors CFIUS should consider.

The Order elaborates on two existing statutory factors—supply chain resiliency and technological leadership—and identifies three additional factors—aggregate industry investment trends, cybersecurity, and American sensitive data.

FACTOR 1 – THE EFFECT ON THE RESILIENCE OF CRITICAL U.S. SUPPLY CHAINS THAT MAY HAVE NATIONAL SECURITY IMPLICATIONS, INCLUDING THOSE OUTSIDE OF THE DEFENSE INDUSTRIAL BASE.

The Order recognizes vulnerabilities created by a particular foreign investment shifting ownership, rights, or control to a foreign person in certain manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security, which may make

the United States vulnerable to supply disruptions of critical goods and services. It further specifies sub-areas of concern, including the following:

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 agricultural industrial base that have implications for food security; and
9. Any other sectors identified in section 3(b) or section 4(a) of Executive Order 14017 (Executive Order on America's Supply Chains), which broadly includes anything identified in two sets of reports published by the Secretaries of Commerce, Energy, Health and Human Services, Defense, Homeland Security, Transportation, and Agriculture (e.g., semiconductor manufacturing and advanced packaging, electric vehicle and other high-capacity batteries, critical minerals and materials, and pharmaceuticals and active pharmaceutical ingredients).[1]

In addition to the Order specifying these areas of concern, it also states that a supply chain threat may be posed not only by certain foreign persons involved in a transaction, but also by relevant third parties tied to that foreign person by a commercial, investment, non-economic, or other relationship. The Order further directs CFIUS to consider factors such as the following:

1. Degree of U.S. supply chain involvement of the relevant foreign person;
2. U.S. capabilities in the specified sectors;
3. Degree of diversification through alternate suppliers, particularly if located in allied or partner economies;
4. Whether the U.S. business in the transaction directly or indirectly supplies the U.S. Government, energy sector industrial base, or defense industrial base; and
5. Concentration of supply chain ownership or control by the relevant foreign person.

FACTOR 2 – THE EFFECT ON U.S. TECHNOLOGICAL LEADERSHIP IN AREAS AFFECTING U.S. NATIONAL SECURITY.

The Order directs CFIUS to consider whether a transaction could reasonably result in future advancements and applications in technology that could undermine national security, presumably by giving a threat actor a technological advantage over the United States. The Order also charges the Office of Science and Technology Policy with periodically publishing a list of sectors fundamental to U.S. technology leadership. Notably, the White House published a Critical and Emerging Technologies List Update on February 7, 2022.

FACTOR 3 – THE EFFECT THAT AGGREGATE INDUSTRY INVESTMENT TRENDS MAY HAVE ON U.S. NATIONAL SECURITY.

Expressing concern regarding incremental investments that may facilitate technology transfers or cede domestic control in certain sectors or technology to a threat actor, the Order directs CFIUS to consider the risks arising from a

transaction in the context of multiple acquisitions or investments in a single sector or in the sectors identified in Factors 1 and 2. The Order also reiterates the potential threat posed by certain foreign and relevant third parties.

FACTOR 4 – THE EFFECT ON U.S. CYBERSECURITY.

The Order directs CFIUS to consider whether a transaction may provide a foreign person or relevant third parties with direct or indirect access to capabilities or information databases and systems so as to enable a threat actor to engage in malicious cyber-enabled activities against U.S interests or persons. It also directs consideration of the cybersecurity posture, practices, capabilities, and access of both the foreign and U.S. parties to the transaction. Some areas of specific concern identified in the Order include the following:

1. The protection or integrity of data in storage or databases or systems housing sensitive data;
2. Interference with U.S. elections, critical infrastructure, the defense industrial base, or other cybersecurity national security priorities in Executive Order 14028 (Executive Order on Improving the Nation's Cybersecurity); and
3. Sabotage of critical energy infrastructure, including smart grids.

FACTOR 5 – THE EFFECT ON U.S. SENSITIVE DATA SECURITY.

The Order directs CFIUS to consider whether foreign investments in U.S. businesses that have access to or store U.S. persons' sensitive data, including health and biological data, involve a foreign person or relevant third parties that may pose a national security threat. It further instructs CFIUS to consider whether such data could be identified or de-anonymized in a manner that could reveal an individual's identity, as well as whether the data may cover a U.S. sub-population that would facilitate targeting of individuals or groups of individuals. Finally, the Order requires CFIUS to consider whether a transaction involves the transfer of U.S. person sensitive data to a foreign person or relevant third parties that may pose a threat.

SUMMARY

Parties considering a transaction involving a U.S. business and a foreign investor or acquirer need to consider the ownership, rights, or control granted to that foreign person. If the transaction falls within CFIUS' jurisdiction and the U.S. business operates in the sectors identified in the Order, the parties need to have a clear understanding of the foreign party or parties involved in the transaction, including any third-party relationships, to assess whether CFIUS could view them as a threat to national security. Finally, the parties should analyze their transaction according to the factors laid out in the Order.

Many transactions falling within the sectors identified in the Order could require a mandatory CFIUS filing. To avoid a potentially significant penalty up to the value of the transaction, it is very important to identify early whether the transaction needs to be filed before closing. Even if a CFIUS filing is not mandatory, the presence of the risk factors specified in the Order may counsel in favor of a voluntary filing. CFIUS has recently emphasized its efforts to find and pursue filings of transactions that were not voluntarily filed with CFIUS. Being pulled into the non-notified process can be costly and operationally disruptive, particularly if it has been several years since closing and CFIUS' review results in a divestment order or heavy mitigation.

Parties enlisting experienced counsel early in the planning process to guide their assessment of a transaction's CFIUS risk profile are not only able to evaluate the need for a filing, but are also better able to structure the transaction and address any potential national security risks to expedite CFIUS' review of a filing. King & Spalding has a global footprint, substantial industry experience, and deep bench of former trade and national security government officials, including a former U.S. Department of Treasury official who recently helped lead the office that chairs CFIUS, and is uniquely positioned to guide companies through a CFIUS analysis.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 23 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE
ATLANTA	CHICAGO	GENEVA	MIAMI	RIYADH	TOKYO
AUSTIN	DENVER	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
BRUSSELS	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	

[1] See our Buy American and Supply Chain Policy Roundup webpage for additional information about Executive Order 14017 and subsequent Executive branch agency reports.