Simpson Thacher

Report from Washington

President Biden Issues Executive Order Memorializing National Security Factors That CFIUS Will Consider

September 15, 2022

To read the White House press release, please click here.

To read the text of the Executive Order, please click here.

On September 15, 2022, President Biden signed a new Executive Order (the "Order") that defines several categories of national security factors that will be considered by the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") when evaluating a transaction. The Order is the first ever Presidential Directive since the Committee's establishment in 1975 to provide formal direction on the risks that must be evaluated by the Committee, and reaffirms the critical role that CFIUS plays in the protection of U.S. national security.

The Order is the first ever Presidential Directive since the Committee's establishment in 1975 to provide formal direction on the risks that must be evaluated by the Committee.

The Order's five categories, discussed in further detail below, touch on topics relating to the integrity of domestic supply chains, the advancement of U.S. technological leadership in key sectors, concentration risk, cybersecurity risks, and sensitive personal data. While the broad sensitivities captured by each factor are already well-known across the CFIUS community and frequently arise as a topics of inquiry, the Order's framework offers a new lens through which parties can address questions and concerns during the course of a review. It should be noted that these factors are intended to be read in conjunction with the existing factors set forth in the Committee's implementing legislation and are illustrative in nature. CFIUS is also encouraged to consider any other national security risks arising out of a transaction.

The Order directs the Committee to evaluate transactions using five factors, with each determination assessing the transaction's effect on the following:

1. *The resilience of critical U.S. supply chains that may have national security implications*. CFIUS has historically maintained an active role in ensuring the continuity of supply chains that support the country's military industrial base. In addition to the Committee's traditional considerations, this factor also calls for evaluation of critical domestic supply chains reaching into other sectors, such as certain manufacturing capabilities, mineral resources, and technologies necessary to avoid disruptions of critical goods and services. We expect this factor to prompt a heightened focus on the entire supply chain for the domestic semiconductor industry ecosystem, in particular.

The Order recognizes that U.S. technological leadership in several key industries remains vital to national security.

2. *U.S. technological leadership in areas affecting national security*. The Order recognizes that U.S. technological leadership in several key industries remains vital to national security. In particular, the Order identifies microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, climate adaptation technologies, and the agricultural industrial base as particularly sensitive, but also recognizes that this list is not intended to be exhaustive. Foreign investment in these and related sectors have been and will continue to be scrutinized closely for signs that the transaction could affect the U.S.'s position in the development of these emerging technologies.
3. *Industry investment trends that may impact national security*. This factor tasks the Committee to consider the concentration risk that may arise as a result of the transaction. In particular, the relative national security risks of the transaction under evaluation may in the abstract be low, but could be much higher if the foreign investor or group of investors from one country has already acquired other similar firms previously. Indeed, the Committee routinely asks questions about the market share of the U.S. business and often requests lists of competitors who may provide similar goods or services. Therefore, it is often prudent to consider as part of a CFIUS analysis an evaluation of the investor's prior investment activity in that sector.
4. *Cybersecurity risks that threaten to impair national security*. The Order requires the Committee to assess whether the transaction may provide a foreign party or other bad actors with the ability to engage in malicious cyber-related activity that could affect national security. While it is clear that foreign parties with any potential ties to cyber criminals will receive some of the highest levels of scrutiny by the Committee, this factor is perhaps more useful when evaluating a U.S. business's cyber-related vulnerabilities and how they may impact national security. Accordingly, CFIUS has expanded its inquiries for critical infrastructure assets in order to understand the IT networks that manage critical systems and how those networks are protected.
5. *Risks to U.S. persons' sensitive data*. A business's access to sensitive personal data of U.S. persons has for several years been a key focus of the Committee, and was recently codified in legislative reforms as an attribute that could trigger a mandatory filing before the Committee. This has been reflected in increased CFIUS attention to investments in companies involved in the insurance, videogame, social media, and education industries. As growing data sets continue to be aggregated and exploited by increasingly powerful tools designed to assist in surveillance, tracking, and targeting individuals or groups, we expect the Committee to continue to scrutinize a foreign party's potential access to any such data held by a U.S. business, but also drill down on the investor's business rationale for partaking in a transaction.

Key Takeaways

While the factors articulated by the Order reflect the Committee's key concerns that arise during the review process and are well-known across the CFIUS community, the Order provides additional clarity into what can often be an opaque process. Non-U.S. investors should continue to expect an increased level of scrutiny for transactions involving U.S. businesses that touch on key domestic supply chains or critical technologies or that present potential cybersecurity risks or have access to the sensitive data of U.S. persons. The Biden Administration's continued focus on the security of domestic supply chains could also portend the development of an outbound foreign investment screening regime.

While the factors articulated by the Order reflect the Committee's key concerns that arise during the review process and are well-known across the CFIUS community, the Order provides additional clarity into what can often be an opaque process.

While the Biden Administration has indicated that the Order is not targeted toward a particular country, it does acknowledge that "some countries use foreign investment to obtain access to sensitive data and technologies for purposes that are detrimental to U.S. national security," and the Order was signed amid growing concerns and heightened U.S. Government scrutiny towards Chinese investments into sensitive industries. And so while the framework is agnostic as to any particular jurisdiction, the Order—when considered under the current political climate—appears to be the latest in a series of efforts by this Administration to address some of the perceived threats that can arise from Chinese investment and influence.

While the framework is agnostic as to any particular jurisdiction, the Order—when considered under the current political climate—appears to be the latest in a series of efforts by this Administration to address some of the perceived threats that can arise from Chinese investment and influence.

While the Order is focused on the CFIUS review process, the factors articulated by the Order are not isolated to CFIUS, but are frequently a focus of many international trade and regulatory regimes such as those administered by sanctions and export control authorities that act as members of the Committee.

Simpson Thacher & Bartlett is experienced in navigating the complexities of the CFIUS review process and continues to monitor the relevant regulatory developments.

For further information about this Report, please contact one of the following members of the Firm's National Security Regulatory Practice:

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Claire Cahoon
+1-202-636-5828
claire.cahoon@stblaw.com
**Not Yet Admitted to D.C. Bar*

Jennifer Ho
+1-202-636-5525
jennifer.ho@stblaw.com

Ryan D. Stalnaker
+1-202-636-5992
ryan.stalnaker@stblaw.com

Malcolm J. (Mick) Tuesley
+1-202-636-5561
mick.tuesley@stblaw.com

Claire M. DiMario
+1-202-636-5536
claire.dimario@stblaw.com

Michael Kalinin
+1-202-636-5989
michael.kalinin@stblaw.com
**Not Yet Admitted to D.C. Bar*

Christine Tillema
+1-202-636-5559
christine.tillema@stblaw.com

Mark B. Skerry
+1-202-636-5523
mark.skerry@stblaw.com

Laurel E. Fresquez
+1-202-636-5537
laurel.fresquez@stblaw.com

Samantha N. Sergent
+1-202-636-5861
samantha.sergent@stblaw.com

NEW YORK CITY

George S. Wang
+1-212-455-2228
gwang@stblaw.com

Daniel S. Levien
+1-212-455-7092
daniel.levien@stblaw.com