Foreign Investment & Trade Alert

Weil

October 3, 2022

From the Bully Pulpit: President Biden Orders CFIUS to Strengthen Its Reviews in Light of Evolving National Security Risks

By Shawn Cooley, Nathan Cunningham, Timothy Welch, Glenda Bleiberg, Christina Carone and William Looney

On September 15, 2022, President Biden issued an Executive Order (the "EO")[1] providing formal instructions regarding the national security factors on which the Committee on Foreign Investment in the United States (the "Committee" or "CFIUS") must focus during its reviews. While an Executive Order initially created CFIUS in 1975, which has been updated several times over the years, this new EO is unique in that it publicly orders CFIUS to do what it is already doing. The stated purpose of this EO is to align "CFIUS' role, actions and capabilities with the Administration's national security priorities" such as preserving U.S. technical leadership, safeguarding sensitive data of Americans, and increasing U.S. supply chain resilience.[2] Notably, the EO does not change CFIUS' preexisting processes or legal jurisdiction, target any country-specific risks, or address any risks posed by outbound investments to countries of concern.

Section 721 of the Defense Production Act of 1950, as amended ("CFIUS' authorizing statute") does not define national security. Rather, the statute provides a non-exhaustive and illustrative list of broad factors CFIUS can consider when it assesses the extent to which any transaction subject to its jurisdiction (i.e., a covered transaction) threatens to impair U.S. national security. Those factors as summarized from CFIUS' authorizing statute include, among other things:

- U.S. domestic production capacity, and long term supply requirements of key energy sources and other critical items;
- Sales of defense and other sensitive products to adversaries of the United States, particularly in the context of a foreign government-controlled transaction;
- U.S. technological leadership in areas affecting U.S. national security;
- Critical technologies and critical infrastructure of the United States;
- Sensitive personal data of U.S. citizens; and
- Information regarding investment trends in the business sectors involved in covered transactions.

Further, for the purposes of CFIUS, "critical technologies" generally refers to:

- Items subject to U.S. dual use and military export controls restrictions;
- Nuclear items, equipment, and facilities; and
- Select agents and toxins.

The EO elaborates on these pre-existing national-security factors and responsibilities, and requires CFIUS to continue to assess the extent to which a covered transaction may impact access to U.S. citizens' personal data, expose or augment certain cyber security risks, and exacerbate potentially problematic investment trends in a particular sector. Specifically, the EO now requires CFIUS to consider five factors for each transaction it reviews. Notably, the EO requires CFIUS to assess the connections of the foreign investor to other foreign persons, including foreign governments, to whom the foreign person has commercial, investment, non-economic, or other ties when CFIUS is ascertaining the extent to which a transaction poses a risk to U.S. national security.

1. The resilience of critical U.S. supply chains that may have national security implications, including those outside of the defense industrial base

While recognizing the importance of cooperating partners and allies to secure supply chains, the EO highlights the significance of this factor by clarifying that it comprises supply chains of critical goods and services (such as manufacturing capabilities, critical mineral resources (e.g., lithium and rare earth elements), or technologies including those essential to chain resilience), outside the defense industrial base. This factor also includes but is not limited to, microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy (including battery storage and hydrogen), climate adaptation technologies, elements of the agricultural industrial base that have effects on food security, advanced packing supply chains, and information communications technology software, data, and associated services (the "Identified National Security Factors"). To that effect, the Committee must consider the degree of involvement of a foreign person or associated third parties to a transaction that might create a threat to U.S national security.

Moreover, CFIUS must consider U.S. capabilities and the degree of diversification through alternative suppliers across the supplier chain, including suppliers located within U.S. allied countries or partners in the sectors/industries describe above. CFIUS must also take into account whether the U.S. business involved in the covered transaction supplies, directly or indirectly, the U.S. Government, the energy sector, industrial base or the defense industrial base and the extent of foreign ownership or control in a particular supply chain.

2. The effect on U.S. technological leadership in the areas affecting U.S. national security

In particular, CFIUS must assess, whether a covered transaction could reasonably result in future advancements and applications in technology, including the Identified National Security Factors, that could weaken national security. Notably, the Office of Science and Technology Policy must publish periodically a list of technology sectors considered fundamental to U.S. technological leadership in areas important to national security in consultation with other members of the Committee, which the EO requires CFIUS to consider during its review of a covered transaction.

3. Aggregate industry investments trends that may have national security consequences

Specifically, CFIUS must consider threats to national security associated with a covered transaction in the context of multiple investments by foreign persons or third parties in a specific sector or relating to manufacturing capabilities, services, critical mineral resources or technology. While CFIUS' authorizing statute does not list the cumulative effect of incremental investments as a factor for CFIUS to consider when conducting its national security risk assessment, CFIUS is required by the statute to include these developments in its annual report to Congress and in practice CFIUS' reviews already account for them. As part of its review, the Committee may ask the International Trade Administration within the Commerce Department for a report analyzing the industry or industries in which the relevant U.S. business operates, and the transaction pattern of and/or cumulative control by a foreign person, directly or indirectly, or a foreign government of a specific industry or sector.

4. Cybersecurity risks that threaten to impair national security

The EO also directs CFIUS to assess whether a covered transaction may provide a foreign person or associated third party with access to conduct cyber intrusions or malicious cyber activities that could pose national security risks. This includes: (i) activities conceived to weaken the integrity or protection of data in storage or databases or systems keeping sensitive data; (ii) activity created with the purpose of interfering with U.S. elections, critical infrastructure, defense industrial base and other cyber securities priorities; and (iii) cybersecurity posture, practices and capabilities of all parties to the transaction that could create a threat to U.S. national security as a result of the transaction.

5. Risks to U.S. persons' sensitive data

The EO reinforces the critical importance of sensitive personal data that may be used for surveillance, tracking, tracing, or targeting an individual or groups of individuals by the foreign investor in the context of recent technological advances and the prevalence of large data sets, which may permit the re-identification or de-anonymization of otherwise unidentifiable data, and commercial or other exploitation of the same. CFIUS must consider whether the transaction concerns a U.S. business that: (i) has access to U.S. persons' sensitive personal data (e.g., health, digital identity, or other biological data) or data than maybe de-anonymized that could be used to trace an individual's identity in a way the threatens national security; (ii) has access to data on U.S. subpopulations that may be used in a way that threatens national security; and (iii) whether the covered transaction entails a transfer of U.S. persons' sensitive personal data to a foreign person that may act to weaken the national security of the U.S. as a result of the transaction. Even though CFIUS' authorizing statute does not expressly list U.S. persons' sensitive data as a factor CFIUS may consider, CFIUS has long considered personal data protection to be a key national security consideration in its standard risk analysis.

Key Takeaways

- Nothing in this EO changes CFIUS' processes or legal jurisdiction and it does not target any country-specific risks.
- In effect, the EO merely transforms CFIUS' pre-existing and robust risk assessment practices into a more structured and required risk assessment process.
- The main objective of the EO appears to offer greater clarity to the private sector about the evolving national security issues on which the Administration and Committee continue to be focused.[3] According to Secretary Janet L. Yellen, who serves as chair of CFIUS, "President Biden's Executive Order highlights CFIUS' increasing attention to national security risks in several key areas and sharpens the Committee's focus on protecting America's national security, while maintaining the U.S. open investment policy."[4]
- Parties to a covered transaction need to prioritize robust CFIUS due diligence as early as possible to effectively identify transactions that are either required to be filed with CFIUS or that otherwise may warrant a voluntary filing with CFIUS after considering these, and other, national security factors.

* * *

[1] Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States, 87 Fed. Reg. 57,369 (Pres. Doc. Sept. 20, 2022).

[2] FACT SHEET: President Biden Signs Executive Order to Ensure Robust Reviews of Evolving National Security Risks by the Committee on Foreign Investment in the United States, available here.

[3] Background Press Call on President Biden's Executive Order on Screening Inbound Foreign Investments, available here.

[4] Statement by Secretary of the Treasury Janet L. Yellen on President Biden's Executive Order on the Committee on Foreign Investment in the United States, available here.

If you have questions concerning the contents of this alert, or would like more information, please speak to your regular contact at Weil or to the authors:

Authors

Shawn Cooley (D.C.)	View Bio	shawn.cooley@weil.com	+1 202 682 7103
Nathan Cunningham (D.C.)	View Bio	nathan.cunningham@weil.com	+1 202 682 7156
Timothy Welch (D.C.)	View Bio	timothy.welch@weil.com	+1 202 682 7132
Glenda Bleiberg (D.C.)	View Bio	glenda.bleiberg@weil.com	+1 202 682 7016
Christina Carone (D.C.)		christina.carone@weil.com	+1 202 682 7258
William Looney (D.C.)	View Bio	william.looney@weil.com	+1 202 682 7143