September 20, 2022

Executive Order Providing Guidance to CFIUS on Evolving National Security Risks

President Biden Provides Formal Direction to CFIUS on Supply Chains, Investment Trends, and Other Risk Factors

SUMMARY

On September 15, 2022, President Joseph R. Biden issued an Executive Order (the "EO") stressing the importance of ensuring that the foreign investment review process in the United States remains responsive to an evolving national security landscape, while at the same time reaffirming that the United States welcomes and supports foreign investment – consistent with the protection of national security. To that end, the EO directs the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") to consider five specific risk factors when it reviews a transaction.[1] The EO provides direction to CFIUS to ensure that its review of covered transactions remains responsive to evolving national security risks, including, as a technical matter, by elaborating and expanding on the risk factors identified in subsections (f)(1)-(10) of section 721 of the Defense Production Act of 1950, as amended (50 U.S.C. 4565). Much of what the EO sets forth is already considered by CFIUS in its review of covered transactions, but the EO prescribes a more formal analytical framework. The EO is the first time since the executive order establishing CFIUS in 1975 that a President has used the executive order mechanism to provide formal Presidential direction on the risks that CFIUS should assess in its evaluation of covered transactions.[2]

The EO adds an emphasis, already a topic of focus for the Biden Administration, on climate adaptation technologies, critical materials, and food security, to the enumerated factors to be considered by CFIUS. Fundamentally, however, other than this renewed emphasis, the content of the EO does not break new ground, as CFIUS already considers most, if not all, of these factors in its review of transactions. The timing of CFIUS review generally should not be impacted, although it is possible that certain transactions that touch on the areas of focus specified in the EO could take longer to clear than they might have prior to the issuance of the EO. Even though the EO does not necessarily break new ground, the EO approach is novel

in its recognition of the need to stay ahead of evolving risks and in its express and public recognition of these factors.

The risk factors identified in the EO do not replace current CFIUS risk considerations, but rather elaborate upon and expand the statutory factors[3] specified in 50 U.S.C. § 4565(f), as well as additional informal factors, that CFIUS already considers in its review of covered transactions.[4] The EO thus emphasizes certain factors that the President deems to be of particular importance in light of the evolving national security landscape and the evolving nature of the investments that may pose risks to national security, but the risks identified in the EO do not exhaust the risks that CFIUS may consider when reviewing a covered transaction, and the Biden Administration expressly emphasized that CFIUS "may consider any national security risk arising out of a transaction over which it has jurisdiction."[5]

FIVE SETS OF RISK FACTORS THE EO DIRECTS CFIUS TO CONSIDER

In its press release, the Administration ties the EO to its broader foreign policy objectives: "preserving U.S. technological leadership, protecting Americans' sensitive data, and enhancing U.S. supply chain resilience."[6] These objectives animate the five specific sets of risks factors the EO identifies for CFIUS attention:

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."***[7] As certain foreign investment may undermine supply chain resilience efforts and therefore national security by making the United States vulnerable to future supply disruptions, the EO directs CFIUS to consider when "an investment shifts ownership, rights, or control with respect to certain manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security" to a foreign person who might take actions that threaten to impair the national security of the United States as a result of the transaction, or to other foreign persons, including foreign governments, to whom the foreign person has commercial, investment, non-economic, or other ties that might cause the transaction to pose a threat to U.S. national security.[8] The EO instructs CFIUS to evaluate, among other things, and as appropriate, (i) the effect of the proposed transaction on supply chain resilience and security, both within and outside the defense industrial base, in manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security;[9] (ii) the United States capability with respect to manufacturing capabilities, services, critical mineral resources, or technologies, including those that are fundamental to national security; (iii) the degree of involvement in the United States supply chain by a foreign person who is a party to the covered transaction and who might take actions that threaten to impair the national security of the United States as a result of the transaction, or who might have relevant third-party ties that might cause the transaction to pose a threat; (iv) the degree of diversification through alternative suppliers across the supply chain, including suppliers located in allied or partner economies, and the concentration of ownership or control by the foreign person in a given supply chain; and (v) whether the United States business that is party to the covered transaction supplies, directly or indirectly, the United States Government, the energy sector industrial base, or the defense industrial base.
2. ***"A given transaction's effect on U.S. technological leadership in areas affecting U.S. national security[.]"***[10] The EO notes that although in many cases foreign investments can help to foster domestic innovation, it is important to protect United States technological leadership by addressing the risks posed by investments by foreign persons who might take actions that threaten to impair the national security of the United States as a result of the transaction, and by

addressing whether such persons have relevant third-party ties that might cause the transaction to pose such a threat. Accordingly, the EO directs CFIUS to consider, as appropriate, whether a covered transaction involves manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to United States technological leadership and therefore national security, such as microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies.[11] CFIUS is also directed to consider, as appropriate, relevant third-party ties that might cause such a transaction to threaten to impair the national security of the United States, and whether the transaction "could reasonably result in future advancements and applications in technology that could undermine national security."[12]

3. ***"Aggregate industry investment trends that may have consequences for an individual transaction's impact on U.S. national security."***[13] The concern here is that incremental investments over time may result in national security risk, even if no single transaction does. In other words, a series of acquisitions in the same, similar, or related United States businesses involved in activities that are fundamental to national security or on terms that implicate national security may result in a particular covered transaction giving rise to a national security risk when considered in the context of transactions that preceded it.[14] The EO seeks to ensure that CFIUS considers this context in order to prevent the weakening of U.S. domestic capabilities in an incremental manner.[15] To that end, the EO directs CFIUS, as appropriate, to consider the cumulative effect of individual transactions to avoid an aggregation that facilitates a harmful technology transfer to foreign persons in sectors or technologies crucial to U.S. interests.[16] The EO states that in order to assist its review, the Committee may request the Department of Commerce's International Trade Administration to provide an analysis that details "the cumulative control of, or pattern of recent transactions by, a foreign person" of the sector in which the relevant U.S. business operates.[17]

4. ***"Cybersecurity risks that threaten to impair national security."***[18] The EO stresses that it is important to ensure that foreign investment in United States businesses does not erode United States cybersecurity, as investments by foreign persons with the capability and intent to conduct cyber intrusions or other malicious cyber-enabled activity – such as activity designed to affect the outcome of any election for Federal, State, Tribal, local, or territorial office; the operation of United States critical infrastructure; or the confidentiality, integrity, or availability of United States communications – may pose a risk to national security. Thus, the EO directs CFIUS to consider, as appropriate, whether a covered transaction might provide direct or indirect access to capabilities or information databases and systems that would allow a foreign person or related parties to engage in cyber activities that threaten U.S. national security.[19] Specifically, the EO identifies the risks that a covered transaction could lead to activity designed to undermine the protection or integrity of data in storage or databases or systems housing sensitive data; election interference; harm to critical infrastructure, such as the sabotage of smart grids; threats to the defense industrial base; and harm to any of the cybersecurity priorities articulated in Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity).[20] The EO also directs CFIUS to consider, as appropriate, the cybersecurity posture, practices, capabilities, and access of both the foreign person and the United States business that could allow a foreign person who might take actions that threaten to impair the national security of the United States as a result of the transaction, or their relevant third-party ties that might cause the transaction to pose such a threat, to manifest cyber intrusion and other malicious cyber-enabled activity within the United States.

5. ***"Risks to U.S. persons' sensitive data."***[21] Sensitive personal data has been a significant concern of CFIUS for many years. The EO amplifies the national security concerns associated with sensitive personal data, including that data is an increasingly powerful tool for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals. The EO also states that it is important for the United States Government to stay current with threats posed by advances in data processing and evaluation technology, including by considering potential risks posed by foreign persons who might exploit access to certain data regarding United States persons to target individuals or groups within the United States to the detriment of national

security. In particular, the EO highlights and directs CFIUS to assess, as appropriate, risks stemming from covered transactions where a foreign person or related parties might threaten U.S. national security by gaining access to U.S. health and biological data; U.S. digital identities; data that was once unidentifiable but that could be re-identified or de-anonymized due to advances in technology; and data on U.S. sub-populations.[22]

CFIUS TO PERIODICALLY REVIEW ITS APPROACH

The EO requires CFIUS to review its "processes, practices and regulations" to ensure its consideration of risk reflects current national security threats.[23] The Committee is also to periodically provide the Assistant to the President for National Security Affairs a report documenting the results of this review, including any resulting policy recommendations that CFIUS considers necessary to meet the evolving set of national security risks.[24]

CONCLUSION

In response to the CFIUS report or as other evolving trends materialize, additional EOs might impose further innovations on CFIUS practice. Developments should be monitored, and transaction parties should be particularly sensitive to the risk factors identified in the EO, as they are likely to be top of mind for CFIUS in the near term.

* * *

ENDNOTES

1 *Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States*, THE WHITE HOUSE BRIEFING ROOM (Sep. 15, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/09/15/executive-order-on-ensuring-robust-consideration-of-evolving-national-security-risks-by-the-committee-on-foreign-investment-in-the-united-states.

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*, THE WHITE HOUSE BRIEFING ROOM (Sept. 15, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/15/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.

3 Fact Sheet, *supra* note 2.

4 50 U.S.C. § 4565(f) states, "Factors to be considered — For purposes of this section, the President or the President's designee may, taking into account the requirements of national security, consider-- (1) domestic production needed for projected national defense requirements, (2) the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials, and other supplies and services, (3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security, (4) the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to any country-- (A) identified by the Secretary of State-- (i) under section 4605(j) of this title, as a country that supports terrorism; (ii) under section 4605(l) of this title, as a country of concern regarding missile proliferation; or (iii) under section 4605(m) of this title, as a country of concern regarding the proliferation of chemical and biological weapons; (B) identified by the Secretary of Defense as posing a potential regional military threat to the interests of the United States; or (C) listed under section 2139a(c) of Title 42 on the 'Nuclear Non-Proliferation-Special Country List' (15 C.F.R. Part 778, Supplement No. 4) or any successor list; (5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security; (6) the potential national security-related effects on United States critical infrastructure, including major energy assets; (7) the potential national security-related effects on United States critical technologies; (8) whether the covered transaction is a foreign government-controlled transaction, as determined under subsection (b)(1)(B); (9) as appropriate, and particularly with respect to transactions requiring an investigation under subsection (b)(1)(B), a review of the current assessment of-- (A) the adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines, which shall draw on, but not be limited to, the annual report on 'Adherence to and Compliance with Arms Control, Nonproliferation and Disarmament Agreements and Commitments' required by section 2593a of Title 22; (B) the relationship of such country with the United States, specifically on its record on cooperating in counter-terrorism efforts, which shall draw on, but not be limited to, the report of the President to Congress under section 7120 of the Intelligence Reform and Terrorism Prevention Act of 2004; and (C) the potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations; (10) the long-term projection of United States requirements for sources of energy and other critical resources and material; and (11) such other factors as the President or the Committee may determine to be appropriate, generally or in connection with a specific review or investigation."

5 Fact Sheet, *supra* note 2.

6 *Id.*

7 *Id.*

8 Executive Order, *supra* note 1, Sec. 2(a)(i).

ENDNOTES (CONTINUED)

9 These include: 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, and any other sectors that are identified in section 3(b) or section 4(a) of a prior executive order regarding America's supply chains, Executive Order 14017 of February 24, 2021.

10 Fact Sheet, *supra* note 2.

11 The Office of Science and Technology Policy, in consultation with other CFIUS members, is directed in the EO to periodically publish a list of technology sectors that it assesses are fundamental to United States technological leadership in areas relevant to national security, and CFIUS will consider that list, as appropriate. Executive Order, *supra* note 1, Sec. 2(b)(iv).

12 *Id.* Sec. 2(a)(ii)(B), Sec. 2(b)(ii)-(iii).

13 Fact Sheet, *supra* note 2.

14 Executive Order, *supra* note 1, Sec. 3(a)(i).

15 *Id.*

16 *Id.*

17 *Id.*, Sec. 3(a)(i).

18 Fact Sheet, *supra* note 2.

19 Executive Order, *supra* note 1, Sec. 3 (b)(ii).

20 *Id. See also, Executive Order on Improving the Nation's Cybersecurity*, THE WHITE HOUSE BRIEFING ROOM (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

21 Fact Sheet, *supra* note 2.

22 Executive Order, *supra* note 1, Sec. 3 (c).

23 *Id.*, Sec. 4.

24 *Id.*

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.