GIBSON DUNN

White House Issues First-Ever Executive Order Identifying Additional National Security Factors for CFIUS to Consider in Evaluating Transactions

Client Alert | September 16, 2022

On September 15, 2022, the President issued the first Executive Order ("E.O.") in the nearly 50-year history of the interagency Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") to provide explicit guidance for CFIUS in conducting national security reviews of covered transactions.[1] The E.O. does not legally alter CFIUS processes or legal jurisdiction, but rather elaborates on certain existing factors that the Committee is mandated by statute to consider,[2] and adds further national security factors for the Committee to consider, when it is evaluating transactions. The E.O. comes as the U.S. Government is increasingly focused on strategic competition—particularly regarding the national security implications of critical technologies, critical infrastructure, and sensitive personal data—and builds on the expansive CFIUS authorities codified in the Foreign Investment Risk Review Modernization Act of 2018 and implementing regulations.[3] Importantly, the E.O. continues the momentum established with recent legislation enacted by Congress,[4] as well as other Biden administration initiatives,[5] and comes in the midst of broader discussions about regulating both inbound and outbound technology transfers. This E.O. plays an important role in the U.S. Government approach to achieving national security objectives in protecting U.S. technological competitiveness and curbing U.S. reliance on foreign supply chains involving critical technologies.

Specifically, the E.O. directs CFIUS to consider the following five factors:

- **The resilience of critical U.S. supply chains** that may have national security implications, including those outside of the defense industrial base;
- **U.S. technological leadership** in areas affecting U.S. national security, including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies;
- **Aggregate industry investment trends that may have consequences** for a given transaction's impact on U.S. national security;
- **Cybersecurity risks** that threaten to impair national security; and
- Risks to **U.S. persons' sensitive data**.

We discuss each of these five factors and their impact on the CFIUS process in turn below, as well as the common concern relating to third-party ties highlighted by the E.O. in each of these factors.

The Resilience of Critical U.S. Supply Chains

Related People

Stephenie Gosnell Handler

David A. Wolber

Scott R. Toussaint

With respect to the first factor, the E.O. directs CFIUS to consider supply chain resiliency, inside and outside the defense sector, and whether a transaction could pose a threat of future supply disruptions of goods and services critical to the United States. Specific elements the Committee should consider are whether a supply chain is sufficiently diversified with alternative suppliers including in allied and partner countries, the concentration of ownership or control in the supply chain by the foreign investor, and whether the U.S. party to the transaction supplies to the U.S. Government.

U.S. Technological Leadership

The second factor focuses CFIUS' attention on a transaction's potential effect on U.S. leadership in certain critical sectors that are fundamental to national security, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy and climate adaptation technologies. Not surprisingly, the specific technologies identified in this E.O. align with the most recent list of Critical and Emerging Technologies ("CET") published by the U.S. National Science and Technology Council,[6] in line with the U.S. Government's overall focus on protecting and developing these technologies. Along these lines, part of the CFIUS review of this factor will need to include not only the current state of the U.S. business and technology being acquired, but also now whether the transaction could reasonably result in future advancements and applications in technology that could undermine U.S. national security, according to the E.O.

Consideration of Aggregate Industry Trends

The third factor—directing CFIUS to consider the consequences of industry investment trends on a particular transaction's national security impact—grants the Committee express authority to block a transaction even where the covered transaction itself might not constitute a national security risk. In other words, the assessed national security risk of a covered transaction, standing alone, could be low when viewed on a case-by-case basis. But, under this Presidential direction, CFIUS would also consider broader industry trends, such as whether a specific foreign actor is acquiring or investing in multiple companies in a sector that, in the aggregate, could impact U.S. national security. This factor has significant disruptive potential for deal certainty given that it formally broadens CFIUS review beyond the specific facts of the transaction itself, and we assess this factor and the next (discussed below) to be among the most significant in the E.O. in terms of impact on the CFIUS process.

Cybersecurity Risks

Building on President Biden's E.O. on "Improving the Nation's Cybersecurity,"[7] the fourth factor instructs the Committee to consider whether a covered transaction may provide a foreign person or their third-party ties with access and ability to conduct cyber intrusions or other malicious cyber activity. CFIUS' interest in cybersecurity risks is longstanding; however, this factor appears to give more weight to the growing risk of supply chain compromise that threaten broader national security. This makes sense given the context of the devastating SolarWinds Sunburst attack, in which a malicious nation-state actor leveraged unauthorized access to build a backdoor into a software update for a widely used network monitoring and management software. This backdoor was then used to gain unprecedented access to networks, systems, and data of thousands of organizations—including the U.S. Government. While critical technologies are a well-recognized priority of CFIUS, this factor appears to direct increased attention to technologies that would not necessarily be considered emerging or foundational, but are core to business operations in a manner that could have national security implications should they be compromised by a malicious actor. We therefore anticipate that CFIUS will look more closely at transactions involving the acquisition of basic management systems or software used across key industries and critical sectors, with an emphasis on transactions that may provide a foreign person or their third-party ties with the ability to leverage these systems or software to breach supply chains in those industries and/or

sectors.

Access to U.S. Persons' Sensitive Data

The fifth and final factor in the E.O. directs CFIUS to consider whether a covered transaction involves a U.S. business with access to U.S. persons' sensitive data, and whether the foreign investor has, or the foreign investor's ties have, the ability to exploit that data through commercial or other means to the detriment of U.S. national security. This factor reflects longstanding CFIUS concerns over access to sensitive personal data, and specifically recognizes that the transfer to foreign persons of large data sets can enable foreign persons or countries to conduct surveillance, tracing, tracking, and targeting of U.S. individuals or groups.

A Consistent Theme: National Security Concerns of Third Party Ties

Throughout all five factors, the E.O. directs that CFIUS should be scrutinizing transactions that involve foreign persons with any "third-party ties" which could add to the potential threat to U.S. national security, be it through providing those third parties access to critical technology or the opportunity to disrupt supply chains, engage in malicious cyber activity or misuse U.S. personal data. While no specific third-party ties are identified as riskier than others, it would be no surprise if in the current geopolitical environment ties involving Russia, China and other U.S. strategic competitors would be targeted for enhanced review.

Key Takeaways

In sum, while this is the first-ever E.O. providing guidance concerning the CFIUS review process, most of the direction builds upon the existing policy trendlines of the U.S. Government and the increasing concerns surrounding the national security implications of foreign investments in and acquisitions of U.S. businesses. It is no surprise that advanced technologies, cybersecurity risks, supply chains, and sensitive data remain at the forefront of national security considerations, but this E.O. directs the CFIUS's national security risk analysis in a way that, as a practical matter, will continue to expand the Committee's review authority. It is also being released amidst a series of efforts on the legislative and regulatory fronts to improve the competitiveness and resilience of U.S. technology, including discussions of additional Presidential directives concerning outbound technology transfers and capital, as well as enhanced protections of sensitive personal data. Given this breadth based on the five factors elucidated in the E.O., combined with the Biden administration's goals of prioritizing U.S. competitiveness in certain critical technology sectors, we expect that the number of transactions reviewed by the Committee will continue to grow. Prior to engaging in any M&A activity or investments involving U.S. businesses operating within the sectors implicated by the factors outlined in this week's E.O., transaction parties should carefully assess the likelihood of CFIUS review and the potential need to file a notice or declaration.

---

[1] Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (Sept. 15, 2022), *available at* 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] *See* Section 721(f) of the Defense Production Act of 1950, 50 U.S.C. § 4565(f).

[3] Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232 (2018); 31 C.F.R. Parts 800 to 802.

[4] The CHIPS and Science Act of 2022, recently signed into law by President Biden, is

intended to “ensure the United States maintains and advances its scientific and technological edge,” by “boost[ing] American semiconductor research, development, and production”—”technology that forms the foundation of everything from automobiles to household appliances to defense systems.” The White House, FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China (Aug. 9, 2022), *available at*

https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/.

[5] On September 14, 2022, President Biden announced that the U.S. will invest $40 billion to expand biomanufacturing for key materials needed to produce essential medications, as well as develop and cultivate healthy supply chains to support the advanced development of bio-based materials, such as fuels, fire-resistant composites, polymers and resins, and protective materials. The White House, FACT SHEET: The United States Announces New Investments and Resources to Advance President Biden’s National Biotechnology and Biomanufacturing Initiative (Sept. 14, 2022), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/14/fact-sheet-the-united-states-announces-new-investments-and-resources-to-advance-president-bidens-national-biotechnology-and-biomanufacturing-initiative/.

[6] National Science and Technology Council, Critical and Emerging Technologies Update List (Feb. 2022), *available at* https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

[7] Executive Order on Improving the Nation’s Cybersecurity (May 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

The following Gibson Dunn lawyers prepared this client alert: Stephenie Gosnell Handler, David A. Wolber, Annie Motto, Scott Toussaint, and Claire Yi.

Gibson Dunn’s lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following members and leaders of the firm’s International Trade practice group:

United States Judith Alison Lee – Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, jalee@gibsondunn.com) Ronald Kirk – Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com) Courtney M. Brown – Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com) David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com) Stephenie Gosnell Handler – Washington, D.C. (+1 202-955-8510, shandler@gibsondunn.com) Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com) Marcellus A. McRae – Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com) Adam M. Smith – Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com) Christopher T. Timura – Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com) Annie Motto – Washington, D.C. (+1 212-351-3803, amotto@gibsondunn.com) Chris R. Mullen – Washington, D.C. (+1 202-955-8250, cmullen@gibsondunn.com) Samantha Sewall – Washington, D.C. (+1 202-887-3509, ssewall@gibsondunn.com) Audi K. Syarief – Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com) Scott R. Toussaint – Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com) Shuo (Josh) Zhang – Washington, D.C. (+1 202-955-8270, szhang@gibsondunn.com)

Asia Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com) David A. Wolber – Hong Kong (+852 2214 3764, dwolber@gibsondunn.com) Fang Xue – Beijing (+86 10 6502 8687, fxue@gibsondunn.com) Qi Yue – Beijing – (+86 10 6502 8534,

qyue@gibsondunn.com)

Europe Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com) Nicolas Autet – Paris (+33 1 56 43 13 00, nautet@gibsondunn.com) Susy Bullock – London (+44 (0) 20 7071 4283, sbullock@gibsondunn.com) Patrick Doris – London (+44 (0) 207 071 4276, pdoris@gibsondunn.com) Sacha Harber-Kelly – London (+44 (0) 20 7071 4205, sharber-kelly@gibsondunn.com) Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com) Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com) Michael Walther – Munich (+49 89 189 33 180, mwalther@gibsondunn.com) Richard W. Roeder – Munich (+49 89 189 33 115, rroeder@gibsondunn.com)

Related Capabilities

International Trade Advisory and Enforcement