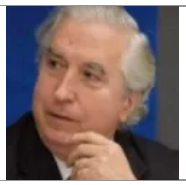
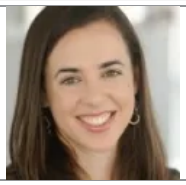


Twitter v. Musk: Where Are the Arbs?

By John C. Coffee, Jr.

Asset Managers as Regulators

1 *By Dorothy S. Lund*



Reforming the Macroprudential Regulatory Architecture in the United States

By Kathryn Judge and Anil Kasi

Editor-At-Large
Reynolds Holding

THE CLS BLUE SKY BLOG

COLUMBIA LAW SCHOOL'S BLOG ON CORPORATIONS AND THE CAPITAL MARKETS

Editorial Board
John C. Coffee, Jr.
Edward F. Greene
Kathryn Judge

Skadden Discusses Executive Order on CFIUS Authority to Identify National Security Risks

By Brian J. Egan, Michael E. Leiter and Ondrej Chvosta September 19, 2022

Comment

On September 15, 2022, President Joe Biden issued an executive order (EO) "on ensuring robust consideration of evolving national security risks" by the Committee on Foreign Investment in the United States (CFIUS or the Committee). The EO does not change CFIUS jurisdiction or process, nor does it, as a practical matter, materially change the factors CFIUS regularly considers (or has considered over the past several years) when reviewing a CFIUS filing for national security risk. Despite the EO's modest changes to policy, its articulation of some specific areas of concern may have a marginal effect on CFIUS agencies' future reviews and reinforces the experience of regular CFIUS participants: The Committee retains extraordinary discretion to define and mitigate national security risks as it sees fit.

Importantly, this EO may only be the first in a series of consequential executive branch actions on trade and investment that focus on national security. More specifically, expected developments relating to outbound investment review,[1] amending and clarifying regulations governing the importation of information communications and technology services (ICTS),[2] and further updating export controls involving foundational and emerging technologies remain on the Biden administration's "to do" list. And while both today's EO and future steps are largely motivated by concerns related to China, these yet-to-be finalized steps portend significantly greater disruption to a range of investment and commercial activities.

National Security Review Factors Articulated by the EO

CFIUS' mandate is to review covered investment and real estate transactions in the United States for national security risks. The CFIUS statute — Section 721 of the Defense Production Act of 1950, as amended (the DPA) — includes a list of national security factors for the Committee to consider in its review of transactions, while also providing the Committee with the discretion to review "such other factors as the President or the Committee may determine to be appropriate."

The EO expands upon two national security factors in the DPA and directs CFIUS to consider three additional national security factors, discussed in more detail below, which focus on supply chain resiliency, U.S. technological leadership, aggregate investment trends, cybersecurity and sensitive data, respectively. These factors track closely what has been integral to CFIUS' practice since the adoption of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). In addition — and as has been the Committee's practice for many years prior — the EO reinforces CFIUS' broad authority and significant discretion to identify national security factors as it deems appropriate.

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

Although the DPA already directs CFIUS to consider the impact on national security of "the control of domestic industries and commercial activity," the EO makes clear that U.S. supply chains should be a focus of CFIUS' review both inside and outside of the defense/military context. In assessing a transaction's impact on the supply chain, factors for consideration include the degree of diversification through alternative suppliers across the supply chain and supply relations with the U.S. government, with the energy industry and with the defense industry. Significantly, the EO specifically lists "concentration of ownership or control by the foreign person in a given supply chain" as a factor, which seems to invite an antitrust-style analysis. Consequently, examining supply chains during transactional due diligence will continue to be crucial when parties assess whether a voluntary filing is warranted or whether their transaction is likely to be cleared with or without mitigation. Moreover, an issue relating to the supply chain that may be commercially insignificant may nevertheless prove material from CFIUS' standpoint.

A given transaction's effect on 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"

This factor, which expands upon the DPA requirement to consider U.S. "international technological leadership in areas affecting U.S. national security," validates CFIUS' existing approach to national security and advanced technologies, which includes areas beyond defense and critical infrastructure needs. This factor affirms that U.S. "technological leadership" in *any* industry can be considered a matter of national security. The EO further instructs CFIUS to consider whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine national security. The EO requires the Office of Science and Technology Policy (OSTP) 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 directs OSTP to "draw on the findings of other United States Government efforts."

The EO's list of "fundamental" technology sectors closely tracks requirements in the Export Control Reform Act of 2018 (ECRA), a corollary piece of legislation passed with FIRRMA that required the Department of Commerce to identify and establish export controls for foundational technologies or technologies "essential to national security," including those "essential to innovation." Importantly, however, while the EO lists "fundamental" technologies to which CFIUS will be particularly sensitive, these technology areas will not trigger statutorily required CFIUS changes (*i.e.*, mandatory filings and jurisdiction over noncontrolling investments) unless and until the Department of Commerce issues corresponding export controls required under ECRA.

Industry investment trends that may have consequences for a given transaction's impact on U.S. national security

For the first time CFIUS has clear direction to look beyond the four corners of a specific transaction in conducting a review to consider broader "investment trends" in an industry. FIRRMA established this principle in the "sense of Congress" section rather than as a stand-alone review factor. When viewed in isolation, a single investment may appear to pose only limited threat, but when viewed in the context of a "series of acquisitions in the same, similar, or related United States businesses involved in activities that are fundamental to national security," the potential threat may be materially greater. This factor is also considered in the context of supply chain risks and the concentration of control typically reserved for competition authorities to analyze.

Cybersecurity risks that threaten to impair national security

The EO expands on another "sense of Congress" provision from FIRRMA in directing CFIUS to consider cybersecurity risks presented by the transaction under review. The EO also instructs CFIUS to consider, as appropriate, the cybersecurity posture, practices, capabilities and access of not only the foreign investor but also the U.S. business. This reflects CFIUS' ongoing focus not only on the foreign person's opportunity or ability to exploit cyber vulnerabilities in U.S. businesses, but also the capacity of third-party actors related to the foreign person to do so. In addition, since the SolarWinds cybersecurity breach in early 2020, we have seen (and expect we will continue to see) CFIUS give particular attention to cybersecurity vulnerabilities and risks posed by third-party vendors that work with U.S. government contractors.

Risks to U.S. persons' sensitive data

Although CFIUS has always considered any personal data collection by a target to be sensitive, the EO suggests that the definition of "sensitive personal data," as the term is used in FIRRMA implementing regulations, should be interpreted only as a jurisdictional consideration. Other types and sets of data — even if they do not meet the definition of "sensitive personal data" or relevant volume thresholds — may be the focus of a covered transaction's review. CFIUS' concern centers around advances in technology that, combined with access to large data sets, increasingly enable the reidentification or "de-anonymization" of what once was unidentifiable data.

Conclusion

Though some of the newly articulated factors in the EO are likely to further encourage members of CFIUS to broaden their analysis and review, the factors themselves have already been an integral part of the CFIUS review dynamic established by FIRRMA. At this early stage, we do not expect the EO will radically change the outcomes we have seen over the past several years; however, it may increase mitigation on the margins and empower some agencies to play a larger role in regulating areas that are less traditionally considered part of "national security." Perhaps, however, the EO's greatest significance is in what it didn't address: outbound investment reviews, implementation of broad-reaching ICTS controls and a more aggressive push on long-delayed export control reforms. Given continued bipartisan support for managing relations with China, we expect developments on each of these fronts in the coming months.

ENDNOTES

1 *See* our June 21, 2022, client alert "Congress Reportedly Advances Broad Proposal for Outbound Screening of US Investments in Identified Countries of Concern, Including China."

2 *See* our January 19, 2022, client alert "Security Concerns Prompt Multiple Supply Chain Initiatives."

This post comes to us from Skadden, Arps, Slate, Meagher & Flom LLP. It is based on the firm's memorandum, "Executive Order Reinforces CFIUS' Broad Authority To Identify National Security Risks," dated September 16, 2022, and available here.

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Post Comment