

Key Takeaways From President Biden's Executive Order 14083 on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States ("CFIUS")

by Justin T. Huff, Lawrence Ward, T. Augustine Lo, and Dave Townsend

On September 15, 2022, President Biden issued Executive Order 14083 ("EO 14083") that the White House describes as a "first-ever presidential directive defining additional national security factors for CFIUS to consider in evaluating transactions." Rumors of its publication have been circulating in Washington, D.C. for months, and for those that follow foreign investment activity in the United States, it is revealing any time the Executive Branch speaks publicly about CFIUS.

Below we provide a few insights into how EO 14083 will affect the CFIUS transactional review process going forward and the additional considerations U.S. businesses anticipating foreign investment should evaluate early in their deal lifecycles.

The United States retains its open investment policy. The Biden Administration reaffirmed that the United States is open to foreign investment and that the United States recognizes the economic benefits that foreign capital provides to "economic growth, productivity, competitiveness, and job creation." Thousands of companies each year benefit from foreign investments and, relatively speaking, only a handful of transactions present unacceptable risks to national security, as determined by CFIUS. As we have discussed previously, CFIUS regularly faces the challenging task of identifying those transactions that threaten U.S. national security in an ever-changing landscape.

CFIUS will have new factors to consider in its transaction reviews. EO 14083 directs CFIUS to consider five specific groups of factors when reviewing foreign investment in U.S. businesses. These include:

- A transaction's effect on U.S. supply chain resilience and security, both within and outside the American defense industrial base;
- A transaction's effect on U.S. technological leadership in certain areas including but not limited to microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies;

Related People

- Justin T. Huff
- Lawrence Ward
- T. Augustine Lo
- Dave Townsend

Related Capabilities

- Asia-Pacific
- Corporate Governance & Compliance
- Government Enforcement & Corporate Investigations
- Investment Management
- Mergers & Acquisitions
- National Security Law

- Industry investment trends by a particular investor or group of investors from the same country within a specific industry or sector;
- Cybersecurity risks that threaten to impair national security, including potential risks to national elections, critical infrastructure, or critical energy infrastructure, including smart grids; and
- Transactions that may put at risk U.S. persons' sensitive data, including health, digital identity, or other biological data.

These highlighted factors will not replace the existing national security factors CFIUS already considered that are included in CFIUS's regulations but should rather serve as an illustrative focus list. EO 14083 recognizes the evolving national security landscape and directs the White House Office of Science and Technology Policy ("OSTP"), in consultation with other CFIUS member agencies, to publish periodically a list of additional technology sectors that it assesses are fundamental to U.S. technology leadership in areas relevant to national security. Although investments within such enumerated sectors identified in EO 14083 (or later by OSTP) will face increased scrutiny, CFIUS has found, and will likely continue to find, national security risks across all sectors of the U.S. economy as vulnerabilities and threats evolve.

CFIUS is unlikely to shift radically from how it currently operates. EO 14083 provides public insight into how CFIUS operates and some of the key factors that CFIUS has considered for years. Many of these factors are familiar to companies and practitioners that have had their transactions reviewed by CFIUS.

For example, the U.S. government views threats to cybersecurity and U.S. persons' sensitive data as unacceptable and will use every authority available to protect such information. CFIUS had closely scrutinized semiconductor, biotechnology, and artificial intelligence deals even before Congress passed the Foreign Investment Risk Review Modernization Act ("FIRRMA") in 2018, and certain transactions involving these types of U.S. businesses are already be subject to FIRRMA's mandatory notification requirements. However, because CFIUS does not disclose detailed information regarding the transactions it reviews, companies are unable to assess properly whether their investment into a specific sector will be prohibited because CFIUS perceives that there has already been "too much" foreign investment in a particular sector.

EO 14083 directs CFIUS to implement this new guidance consistent with CFIUS's statutory mandate to determine the effect on national security for each transaction it reviews. As such, CFIUS likely will revise its current regulations to include the new EO 14083 directives.

The U.S. Government will apply coordinated efforts across agencies to ensure U.S. leadership in key sectors of the American economy. EO 14083 represents a continued effort by the U.S. Government to ensure American technological leadership in areas that affect U.S. national security. Prior EOs, such as EO 13873 issued on May 15, 2019, titled *Securing the Information and Communications Technology and Services Supply Chain* (see our earlier update [here](#)), and statutes like FIRRMA and the recently passed CHIPS Act (as discussed [here](#)), have all been intended to enhance U.S. national

security. EO 14083 will thus extend that longstanding U.S. industrial policy objective and reinforce the Government's continued commitment to the primacy of national security and ensuring future American scientific and technological leadership in critical sectors.