

Alert

September 21, 2022



Biden Administration Significantly Expands CFIUS National Security Factors

Biden Administration Significantly Expands CFIUS National Security Factors

On September 15, 2022, President Biden signed an Executive Order (EO), which connects the work carried out by the Committee on Foreign Investment in the United States (CFIUS or the Committee) to the Administration's national security aims beyond the traditional defense industrial base. This is the first EO of its kind since CFIUS was established in 1975. It comes at a critical time during this Administration's efforts to improve the competitiveness of U.S. technologies and greatly reduce U.S. reliance on foreign supply chains.

CFIUS is an interagency committee chaired by the U.S. Department of the Treasury that reviews foreign investments in U.S. businesses to identify and address U.S. national security concerns. While the EO does not expand CFIUS's underlying jurisdiction or change its processes over covered transactions, it does expand the existing list of factors the Administration believes the Committee should consider when reviewing whether a particular transaction raises U.S. national security concerns. In this regard, the EO proceeds along two related but distinct tracks. First, it elaborates on some of the factors CFIUS currently considers when it reviews a transaction, currently codified at 50 U.S.C. § 4565(f)(1-10)). Second, the EO identifies several new factors that CFIUS must consider in its review of transactions, which may alter the Committee's methods and processes moving forward. While CFIUS is not currently limited by statute in the factors, it may consider when evaluating a particular transaction, the EO signals that certain industries and businesses should now expect heightened regulatory scrutiny.

As it relates to current statutory factors (namely 50 U.S.C. § 4565(f)(3,5)), the EO directs CFIUS to take into account a transaction's effect on U.S. supply chain resilience and security, inside and outside the defense sector, and emphasizes the following manufacturing capabilities, services, critical mineral resources, or technologies as fundamental to national security:

1. Microelectronics;
2. Artificial intelligence;
3. Biotechnology and biomanufacturing;
4. Quantum computing;
5. Advanced clean energy (e.g., battery storage, hydrogen);
6. Climate adaptation technologies;
7. Critical materials (e.g., lithium and rare earth elements); and
8. Agriculture industrial base elements impacting food security.

The EO further advises that the Office of Science and Technology Policy (OSTP), in consultation with CFIUS, will publish a list of technology sectors it considers "fundamental" to the United States' technological leadership in national security areas. These technology sectors will also impact CFIUS's review of transactions in these particular spaces.

The EO also addresses new, additional factors for CFIUS to consider relating to specific issues and industries, as follows.

Aggregate Investment Trends:

- Incremental investments over time in a particular sector/technology that could provide a



Robert K. Magovern

**Co-Vice Chair,
Transportation
& Trade**

rmagovern@cozen.com
Phone: (202) 463-2539
Fax: (202) 912-4830



Matthew J. Howell

Associate

mhowell@cozen.com
Phone: (202) 912-4879
Fax: (202) 499-2451

Related Practice Areas

- Corporate
- Real Estate
- Trade Regulation, Export Controls & Sanctions
- Transportation & Trade

foreign person with the ability to threaten to impair U.S. national security;

- Risks arising from a single transaction when taken in the context of multiple acquisitions/investments in a particular category (manufacturing capabilities, services, critical mineral resources, etc.).

Cybersecurity Risks:

The EO directs CFIUS to consider the following factors as to whether a covered transaction may provide a foreign person with access to capabilities or information systems that could harm U.S. interests:

- Activity designed to undermine protection/integrity of systems housing sensitive data;
- Activity designed to interfere with U.S. elections, critical infrastructure, or other cybersecurity national security priorities;
- The sabotage of critical energy infrastructure (e.g., smart grids);
- The cybersecurity posture, practices, and capabilities of the foreign person and U.S. business, and whether such issues could manifest in cyber intrusion within the United States.

Risks to U.S. Persons' Sensitive Data:

- Whether foreign investments in U.S. businesses with access to (or storage of) U.S. persons' health and biological data involve a foreign person who may take action to threaten the United States;
- Whether the U.S. business:
 - Has access to U.S. persons' sensitive data (e.g., health, digital identity, biological data, or other data that could trace an individual's identity);
 - Has access to data on "sub-populations" in the United States that could target individuals or groups;
 - Whether a covered transaction results in a transfer of U.S. persons' sensitive data to a foreign person.

With respect to each of the above factors, the EO directs CFIUS to evaluate whether the foreign party has commercial, investment, non-economic, or other ties with foreign governments that might cause the transaction in question to pose a threat to national security.

As indicated in its recent Annual Report, CFIUS continues to review transactions at an increasing rate and in a variety of industries. The new review factors in this EO, along with this Administration's clear priorities in promoting U.S. competitiveness in numerous business sectors, further illustrate that the number of transactions reviewed by CFIUS will grow. Foreign parties and U.S. businesses considering mergers, acquisitions, or investments in any of the sectors identified in the EO should carefully consider the need to seek CFIUS pre-clearance as part of any proposed transaction.
