THE WHITE HOUSE
WASHINGTON

September 15, 2022

EXECUTIVE ORDER

- - - - - - -

ENSURING ROBUST CONSIDERATION OF EVOLVING NATIONAL SECURITY RISKS BY THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

By the authority vested in me as President by the Constitution and the laws of the United States of America, including section 721 of the Defense Production Act of 1950, as amended (50 U.S.C. 4565) (section 721), and section 301 of title 3, United States Code, it is hereby ordered as follows:

Section 1. Policy. The United States welcomes and supports foreign investment, consistent with the protection of national security. The United States commitment to open investment is a cornerstone of our economic policy and provides the United States with substantial economic benefits, including "the promotion of economic growth, productivity, competitiveness, and job creation, thereby enhancing national security," as the Congress recognized in section 1702(b)(1) of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) (Subtitle A of Title XVII of Public Law 115-232). Some investments in the United States by foreign persons, however, present risks to the national security of

the United States, and it is for this reason that the United States maintains a robust foreign investment review process focused on identifying and addressing such risks.

It is important to ensure that the foreign investment review process remains responsive to an evolving national security landscape and the nature of the investments that pose related risks to national security, as the Congress recognized in section 1702(b)(4) of FIRRMA. One factor for the Committee on Foreign Investment in the United States (Committee) to consider, as the Congress highlighted in section 1702(c)(1) of FIRRMA, is that national security risks may arise from foreign investments involving "a country of special concern that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security." Along these lines, I previously underscored in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data From Foreign Adversaries), and emphasize in this order the risks presented by foreign adversaries' access to data of United States persons. With respect to investments directly or indirectly involving foreign adversaries or other countries of special concern, what may otherwise appear to be an economic transaction undertaken for commercial purposes may actually present an unacceptable risk to United States national security due to the legal environment, intentions, or capabilities of the foreign person, including foreign governments, involved in the transaction. It is the policy of the United States Government to continue to respond to these risks as they evolve, including through a robust review of foreign investments in United States businesses.

In light of these risks, this order provides direction to the Committee to ensure that, in reviewing transactions within its jurisdiction (covered transactions), the Committee's review remains responsive to evolving national security risks, including by

elaborating and expanding on the factors identified in subsections (f)(1)-(10) of section 721. This order shall be implemented consistent with the Committee's statutory mandate to determine the effects of each covered transaction reviewed by the Committee on the national security of the United States.

Sec. 2. Elaboration on Existing Statutory Factors.

(a) In considering the factors described in subsection (f)(3) of section 721, the Committee shall, taking into account the requirements of national security, consider the following, as appropriate:

(i) It is important to national security that the Committee continues to assess the effect of foreign investment on domestic capacity to meet national security requirements, including those requirements that fall outside of the defense industrial base. In particular, the resilience of certain critical United States supply chains may have national security implications. The United States recognizes the importance of cooperating with its allies and partners to secure supply chains; however, certain foreign investment may undermine supply chain resilience efforts and therefore national security by making the United States vulnerable to future supply disruptions. These vulnerabilities may occur if 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 -- including because they are critical to United States supply chain resilience -- 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 (relevant third-party ties) that might cause the transaction to pose a threat

to national security).

(ii) The Committee shall consider, as appropriate, the covered transaction's effect on supply chain resilience and security, both within and outside of the defense industrial base, in manufacturing capabilities, services, critical mineral resources, or technologies that are fundamental to national security, including: 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 identified in section 3(b) or section 4(a) of Executive Order 14017 of February 24, 2021 (America's Supply Chains).

(A) The Committee shall consider, as appropriate, 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 such a threat.

(B) The Committee shall consider, as appropriate, the United States capability with respect to manufacturing capabilities, services, critical mineral resources, or technologies, including those described in subsection (a)(ii) of this section; the degree of diversification through alternative suppliers across the supply chain, including suppliers located in allied or partner economies; 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; and the concentration of ownership or control by the foreign person in a given supply chain, among other

factors that the Committee determines to be appropriate in considering whether the covered transaction may undermine the resilience and security of supply chains critical to national security.

(b) In considering the factors described in subsection (f)(5) of section 721, the Committee shall, taking into account the requirements of national security, consider the following, as appropriate:

(i) Although foreign investments can in many circumstances 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.

(ii) The Committee shall 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. The Committee shall also consider, as appropriate, relevant third-party ties that might cause the transaction to threaten to impair the national security of the United States.

(iii) The Committee shall consider, as appropriate, whether a covered transaction could reasonably result in future advancements and applications in technology that could undermine national security.

(iv) The Office of Science and Technology Policy (OSTP), in consultation with other members of the Committee, shall periodically publish a list of technology sectors, including those technologies listed in subsection (b)(ii) of this section, that it assesses are fundamental to United States technological leadership in areas relevant to national security. OSTP shall, as appropriate, draw on the findings of other United States Government efforts to identify technology sectors that are fundamental to United States technological leadership. The Committee shall consider the list described in this subsection, as appropriate.

Sec. 3. Additional Factors to be Considered. (a) In addition to the factors identified in subsections (f)(1)-(10) of section 721, the Committee shall consider, in reviewing the effects of a covered transaction on the national security of the United States, the following factors relating to aggregate industry investment trends that may have consequences for an individual covered transaction's impact on national security:

(i) Incremental investments over time in a sector or technology may cede, part-by-part, domestic development or control in that sector or technology and may give 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, control of or rights in United States businesses in a manner that may result in national security risk. 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. In aggregate, these transactions may facilitate harmful technology transfer in key industries or

otherwise harm national security through the cumulative effect of these investments. As the Congress identified in section 1702(c)(2) of FIRRMA, the Committee may consider "the cumulative control of, or pattern of recent transactions involving, any one type of critical infrastructure, energy asset, critical material, or critical technology by a foreign government or foreign person" in considering national security risks. Contextualizing the Committee's review of an individual transaction in light of the aggregate or series of related transactions could reveal national security risks arising from the covered transaction that were not otherwise apparent.

(ii) The Committee shall consider, as appropriate, as part of the Committee's review of a covered transaction, the risks arising from the covered transaction in the context of multiple acquisitions or investments in a single sector or in related manufacturing capabilities, services, critical mineral resources, or technologies, by any foreign person who might take actions that threaten to impair the national security of the United States as a result of the transaction, or involving relevant third-party ties that might cause the transaction to pose such a threat.

(iii) The Committee may request, as part of the Committee's review of a covered transaction, that the Department of Commerce's International Trade Administration provide the Committee an analysis of the industry or industries in which the United States business operates, and the cumulative control of, or pattern of recent transactions by, a foreign person, including, directly or indirectly, a foreign government, in that sector or industry.

(b) In addition to the factors identified in subsections (f)(1)-(10) of section 721, the Committee shall consider, in reviewing the effects of a covered transaction on the national security of the United States, the following factors relating to cybersecurity risks resulting from a covered transaction that threaten to impair

national security.

(i) It is important for the United States to ensure that foreign investment in United States businesses does not erode United States cybersecurity. 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. The Congress, in section 1702(c)(6) of FIRRMA, identified "exacerbating or creating new cybersecurity vulnerabilities" as a relevant consideration for the Committee when considering national security risks arising from a covered transaction. Review of foreign investment is an important tool as part of broader United States efforts to ensure the cybersecurity of the United States.

(ii) The Committee shall consider, as appropriate, whether a covered transaction may provide 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, with direct or indirect access to capabilities or information databases and systems on which threat actors could engage in malicious cyber-enabled activities affecting the interests of the United States or United States persons, including:

(A) activity designed to undermine the protection or integrity of data in storage or databases or systems housing sensitive data;

(B) activity designed to interfere with United States elections, United States critical infrastructure, the defense industrial base, or other cybersecurity national security priorities set forth in Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity); and

(C) the sabotage of critical energy infrastructure, including smart grids.

(iii) The Committee shall also 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.

(c) In addition to the factors identified in subsections (f)(1)-(10) of section 721, the Committee shall consider, in reviewing the effects of a covered transaction on the national security of the United States, the following factors relating to national security concerns surrounding sensitive data:

(i) Data is an increasingly powerful tool for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security. In section 1702(c)(5) of FIRRMA, the Congress recognized that the Committee may consider whether a covered transaction may "expose, either directly or indirectly, personally identifiable information, genetic information, or other sensitive data of United States citizens to access by a foreign government or foreign person that may exploit that information in a manner that threatens national security." Moreover, advances in technology, combined with access to large data sets, increasingly enable the re-identification or de-anonymization of what once was unidentifiable data. Therefore, it is important for the United States Government to stay current with threats posed by advances in such technology, including by considering potential risks posed by foreign persons who might

exploit access to certain data on United States persons to target individuals or groups within the United States to the detriment of national security. Accordingly, the Committee shall consider whether foreign investments in United States businesses that have access to or that store United States persons' sensitive data, including health and biological data, involve a foreign person who might take actions that threaten to impair the national security of the United States as a result of the transaction, including whether the foreign person might have relevant third-party ties that might cause the transaction to pose such a threat.

(ii) The Committee shall consider, as appropriate, whether a covered transaction involves a United States business that:

(A) has access to United States persons' sensitive data, including United States persons' health, digital identity, or other biological data and any data that could be identifiable or de-anonymized, that could be exploited to distinguish or trace an individual's identity in a manner that threatens national security; or

(B) has access to data on sub-populations in the United States that could be used by a foreign person to target individuals or groups of individuals in the United States in a manner that threatens national security.

(iii) The Committee shall also consider, as appropriate, whether a covered transaction involves the transfer of United States persons' sensitive data 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, and whether the foreign person has relevant third-party ties that have sought to exploit such information or have the ability to exploit such information to the detriment of national security, including through the use of commercial or other means.

Sec. 4. Periodic Review. Consistent with the policy described in section 1 of this order, it is important for the Committee, on an ongoing basis, to continue to review its processes, practices, and regulations, and to continue to make any updates as needed and appropriate to ensure that the Committee's consideration of national security risks remains robust alongside changes to the national security landscape. Accordingly, the Committee shall regularly review its processes, practices, and regulations, and shall periodically provide to the Assistant to the President for National Security Affairs a report documenting the results of its review. The report shall also include any resulting policy recommendations that the Committee considers necessary to meet the evolving set of national security risks.

Sec. 5. Definitions. For purposes of this order, terms shall have the same meanings ascribed to them in section 721 and regulations promulgated by the Committee under section 721.

Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, affect the requirements in section 721 relating to the scope of the Committee's jurisdiction.

(d) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

JOSEPH R. BIDEN JR.

THE WHITE HOUSE,
September 15, 2022.