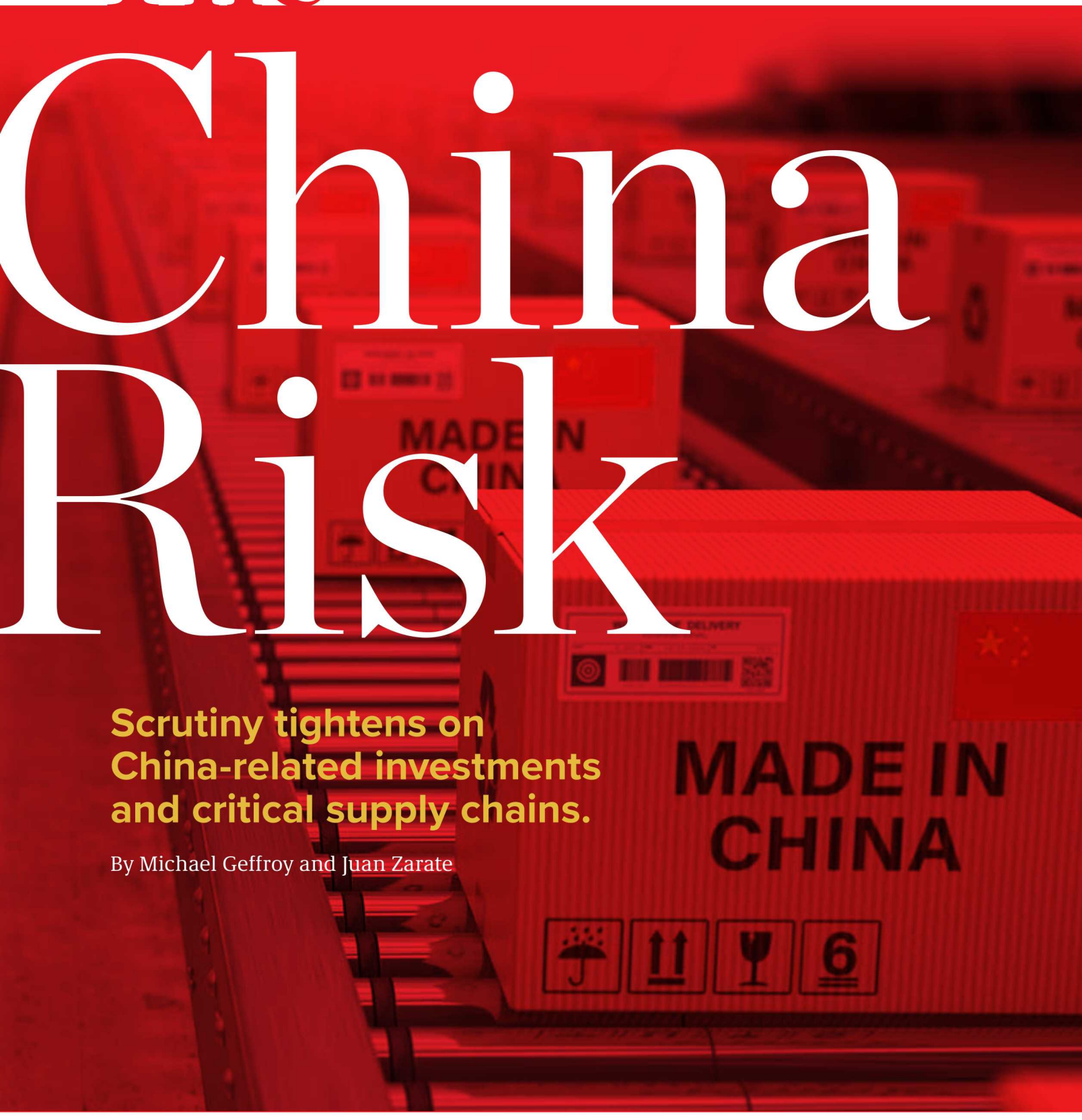
The China Risk



Scrutiny tightens on China-related investments and critical supply chains.

By Michael Geffroy and Juan Zarate

This article was originally published as a K2 Integrity Policy Alert on October 6, 2022. Reprinted with permission. To receive future K2 Integrity Policy Alerts, contact info@k2integrity.com.

The U.S. government continues to increase scrutiny over certain foreign investments in the United States and critical supply chain security. On September 15, 2022, President Biden signed the "Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States" (the CFIUS EO or the EO).[1]

The EO, which details the specific areas where the Biden administration and CFIUS are currently focused, is meant to send "a very clear message, a public message, to the private sector" and to the "corporate community and the public as a whole, as well as foreign governments, allies, and partners around the world."[2]

More recently, the Department of the Treasury released its first-ever Enforcement and Penalty Guidelines (Guidelines) to provide the public with information regarding how CFIUS will assess violations of the laws and regulations that govern transactions and parties subject to CFIUS jurisdiction.[3] A Treasury press release that accompanied the Guidelines included a statement from Assistant Secretary Paul Rosen that "the Committee will not hesitate to use all of its tools and take enforcement action to ensure prompt compliance and remediation, including through the use of civil monetary penalties and other remedies."[4]

Why It Is Important

Given recent legislative and executive actions and broad bipartisan concern in the Congress regarding various threats and risks related to China, both branches of the government will continue to address the national security implications of foreign investments in U.S. businesses and seek to enhance protections around U.S. critical technologies.

The private sector and markets should expect an increasing number of CFIUS reviews and enforcement actions. Also likely are new legislative proposals and presidential directives concerning outbound investments and technology transfers, enhanced protections for personal data of U.S. persons, and an aggressive push for enhanced export controls by the Department of Commerce.[5]

While the EO directs CFIUS to consider certain additional risk factors when reviewing a covered transaction – focusing on the integrity of U.S. supply chains and maintaining U.S. technological leadership – the EO does not expand CFIUS' jurisdiction or its review process. As such, the EO is intended to signal to the public and investors that the Biden administration has prioritized certain areas of national security concern. This is especially true regarding proposed transactions emanating from China.

The EO comes at a time of increasing concern regarding investments from China in the U.S. technology sector and other industries. The private sector has grown more sensitive to Chinese-related investments that could come under CFIUS scrutiny.

Despite this enhanced scrutiny, the 2021 CFIUS annual report published by the Department of the Treasury in August 2022 highlights that investors from China/Hong Kong accounted for the second-largest number of transactions in 2021 (10%), including 44 Notices (16% of all Notices), but just one Declaration (less than 1% of all Declarations).[6]

Overall, the number of filings by Chinese investors increased 105% from 2020 levels (and up 61% from 2019). This represents a notable departure from the trend in recent years, which saw Notices involving Chinese investors decline from 55 in 2018 to 26 in 2019 and just 17 in 2020.

Although the annual CFIUS report does not specify how many China/Hong Kong Notices were approved, the low number of Notices withdrawn and abandoned indicate that CFIUS approved many of the China/Hong Kong Notices (with or without mitigation agreements). Only nine Notices were withdrawn because national security concerns could not be resolved through mitigation agreements.

The jump in Chinese investment is consistent with larger trends concerning the amount of foreign investment in the United States potentially subject to CFIUS review. Foreign direct investment in the United States increased to $4.98 trillion at the end of 2021 from $4.47 trillion at the end of 2020, an increase of $506.1 billion.[7] In 2021, CFIUS saw a significant increase in the number

of filings for covered transactions, reviewing a total of 436 transactions, up from 313 in 2020.

Congress acted to address widespread concerns that Chinese companies improperly obtain critical technologies[8], intellectual property, and other sensitive information from the United States with the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[9] The law expanded the definition of covered transactions subject to mandatory notifications to CFIUS; enhanced the emphasis on mitigation and compliance agreements with transacting parties; and changed the procedures regarding the CFIUS filing process of certain foreign transactions.

Despite FIRRMA's broader reach and expanded notification requirements, the U.S. national security community and Congress remain concerned that foreign investors still use joint ventures and minority stakes in ventures to gain access to sensitive U.S. information and critical technologies.

The EO is part of a larger effort by successive administrations and Congress to enhance supply chain resilience and domestic manufacturing capacity. In addition to FIRRMA, Congress passed the Export Control Reform Act of 2018 (ECRA).[10] ECRA's main initiative is to protect emerging and foundational technologies that are potentially dual-use where there were previously no protections, and where the United States government seeks to ensure that emerging U.S. technologies, and any advantage they may provide, are not seized by foreign countries, especially China, upon export.

The government will continue to address national security implications of foreign investment in U.S. businesses and seek to enhance the protections around U.S. critical technologies. The private sector and markets should expect an increasing number of CFIUS reviews and enforcement actions.

Congress also passed the Creating Helpful Incentives to Produce Semiconductors for America Act of 2022 (the CHIPS Act).[11] This new law establishes investments and incentives to support U.S. semiconductor manufacturing, research and development, and supply chain security. Importantly, the CHIPS Act imposes certain restrictions on the use of the funding and prohibits recipients from expanding semiconductor manufacturing in China and countries defined by U.S. law as posing a national security threat to the United States.[12]

New CFIUS Enforcement Guidelines

On October 20, 2022, the Department of the Treasury released its first-ever Enforcement and Penalty Guidelines (Guidelines).[13] The Guidelines do not provide any new authorities to CFIUS. They are not comprehensive nor binding.[14] They do not impose any new obligations on transacting parties that do not already exist. They do, however, signal how CFIUS will approach compliance and enforcement issues.

The Guidelines describe the types of conduct that may constitute a violation, the sources of information CFIUS relies upon to investigate a potential violation, the penalty process, and specific aggravating or mitigating factors that CFIUS will consider when assessing whether a penalty may be warranted. Importantly, the Guidelines

encourage for the first time the submission of voluntary self-disclosures of conduct that may constitute a violation of the CFIUS laws and regulations.[15]

The Guidelines send the message that CFIUS intends to increase the use of its enforcement powers regarding compliance with mitigation agreements and with mandatory filing regulations, which is consistent with CFIUS' significant increase over the last few years in its staff personnel dedicated to monitoring and enforcement activities.

Considerations for the Private Sector

- The CFIUS EO and Guidelines reflect continued and intensifying concerns about strategically important technologies on a global basis, particularly those put at risk by Chinese investments, and those from other adversaries. Investors and transacting parties should expect more scrutiny concerning Chinese investments, customers, counterparties, and supply vulnerabilities.
- **The CFIUS process is getting more complex.** The Guidelines and the EO's emphasis on the types of transactions that are of particular interest provide clear signals of CFIUS' heightened scrutiny of, and focus on, the privacy of U.S. persons, the protection of critical technologies, and the exclusion of certain geographical areas important to U.S. national security, a concept that CFIUS construes increasingly broadly.
- Transacting parties should take notice of how CFIUS is thinking about compliance and enforcement, and the importance of open and transparent communications with the Committee. **CFIUS will likely be more active in pursuing enforcement actions, which have been limited to date.**[16]
- Those involved in international trade, investments, and mergers and acquisitions need to understand there is a growing suite of national economic security risks and requirements that could impact deals and operations. It is especially important for the investment and technology sectors to understand the fundamental complexities – and potential application and reach – of CFIUS' authority and processes. It is equally important to understand how these interact with export controls and sanctions lists while recognizing how these rules may change in the coming months. Any cross-border investment or acquisition must undergo a rigorous CFIUS assessment.
- Investors and transacting parties should carefully assess how contemplated transactions may be implicated by the areas of risk highlighted by the Biden administration, particularly if these involve the participation of non-U.S. investors. Investing parties should ensure they conduct thorough national security-related diligence on a transaction to anticipate potential CFIUS risks. And, if potential risks are identified, parties should consult with experts to assess potential mitigation terms. Parties that do not notify transactions to CFIUS may be subject to the non-notified process in which CFIUS can request that parties file a transaction after the fact. The downside is that CFIUS may require specific mitigation conditions or even the unwinding of a completed covered transaction.

The recent changes to the law enhancing CFIUS' jurisdiction, the president's EO, and the new Guidelines demonstrate there is a continued and focused interest in the review of foreign investment in the United States at the highest levels of the government, and that CFIUS continues to present increased challenges for foreign investments. These developments will not be the last word on CFIUS, export controls, or foreign investments, whether inbound to, or outbound from, the United States.

Summary of the CFIUS Executive Order

The Defense Production Act sets forth several illustrative factors that CFIUS may consider when assessing whether a "covered transaction" may pose a risk to national security.[17] The EO reinforces those authorities and expands upon two national security factors in the Defense Production Act. The EO also directs CFIUS to consider five additional national security factors:

1. **CFIUS directed to focus on the resilience of critical U.S. supply chains.** Although CFIUS has historically considered supply chains related to the defense industrial base, the

COVID-19 pandemic highlighted weaknesses and dependencies in the U.S. supply chain for a variety of critical goods and inputs, including those outside of the defense industrial base. To address this risk, the EO directs that U.S. supply chains should be a focus of CFIUS reviews both inside and outside the defense context and specifically mentions risks related to food security. This move is one part of a whole-of-government supply chain assessment undertaken by the Biden administration in response to Executive Order 14017.[18] The reference to food security likely is intended to address concern among some lawmakers that the U.S. Department of Agriculture does not have a permanent seat on the committee.

2. **CFIUS directed to focus on U.S. technological leadership in areas affecting U.S. national security.** The EO calls out several sensitive areas critical to maintaining U.S. technological leadership, including microelectronics, artificial intelligence, biotechnology and biomanufacturing, quantum computing, advanced clean energy, and climate adaptation technologies. While CFIUS previously considered the impact of covered transactions on maintaining U.S. technological leadership in critical or emerging technologies, this affirms that leadership in any industry (not just defense) is important to CFIUS. The EO also directs the Office of Science and Technology Policy – a

Investing parties should ensure they conduct thorough national-security related diligence on a transaction to anticipate potential CFIUS risk.

member of CFIUS – to periodically publish a list of technologies that it considers to be fundamental to U.S. technology leadership. This ensures the continued focus going forward of CFIUS on transactions involving specified emerging and critical technologies.

3. **CFIUS directed to consider aggregate investment activity in particular industries.** The EO directs CFIUS to consider a covered transaction in the context of other investments in that same sector. This new directive requires CFIUS to analyze investment trends that may have consequences for a given transaction's impact on U.S. national security. An example might be, "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." Although CFIUS previously considered transactions on a case-by-case basis, this direction gives CFIUS a new responsibility to look beyond single transactions to consider broader, systemic threats to an industry. As such, CFIUS may seek to incorporate industry-level analyses in its risk assessments more frequently.
4. **CFIUS directed to consider cybersecurity risks that threaten to impair national security.** The EO directs CFIUS to consider the impact of a covered transaction on the cybersecurity of the United States. This includes whether the covered transaction would permit a foreign person or third parties with access to sensitive data or systems. In addition, the EO also directs CFIUS to consider the cybersecurity posture, practices, capabilities, and access of the U.S. business. This reflects CFIUS' ongoing focus on risks that may arise in relation to third-party vendors that may provide a foreign person with unauthorized access to sensitive data or systems of a U.S. business.[19]
5. **CFIUS directed to consider risks to U.S. persons' sensitive data.** The EO directs CFIUS to consider whether a covered transaction involves a U.S. business with access to U.S. persons' sensitive data, an area of potential risk that CFIUS has previously focused on in several high-profile cases, such as TikTok.[20] CFIUS is increasingly concerned about any kind of personal data of U.S. persons, even if the volume of data does not reach the threshold of "sensitive personal data" under the FIRRMA's implementing regulations. Going forward, CFIUS will consider the ability to exploit that data through commercial or other means to the detriment of U.S. national security in the context of recent technologies that are able to de-anonymize personal data via gathering and analyzing large data sets. **CM**

The Honorable **Juan Zarate** is Global Co-managing Partner and Chief Strategy Officer at K2 Integrity. He is the Chairman and Co-founder of Consilient. He served as the deputy assistant to the president and deputy national security adviser for combating terrorism (counterterrorism czar), and was the first-ever assistant secretary of the treasury for terrorist financing and financial crimes. He also was a federal terrorism prosecutor. Zarate is the Chairman of the Center on Economic and Financial Power at the Foundation for the Defense of Democracies, and Senior Advisor at the Center for Strategic and International Studies. He was a visiting lecturer at the Harvard Law School and is a published author, including the books *Treasury's War* (2013) and *Forging Democracy* (1994).

Michael Geffroy is an Associate Managing Director at K2 Integrity. He served as Senior Vice President in HSBC Bank USA, N.A.'s Office of Public Affairs. He was General Counsel for the U.S. Senate Select Committee on Intelligence (2014-2017), and Deputy Staff Director and Chief Counsel to the House Committee on Homeland Security (2013-2014). Geffroy also served as the Assistant Director for Enforcement at the Department of the Treasury's Office of Foreign Assets Control. Previously, he served as Counselor to the Assistant Attorney General of the Criminal Division of the Department of Justice, and as an Assistant U.S. Attorney in the District of Columbia.

ENDNOTES

1 Executive Order on Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (15 September 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/. It is the first-ever related Executive Order since the Committee on Foreign Investment in the United States (CFIUS or the Committee) was established in 1975. CFIUS is an interagency committee currently drawn from 16 departments and agencies that reviews foreign investments in U.S. businesses, identifying and addressing U.S. national security concerns. CFIUS has the authority to initiate reviews of "covered transactions," suspend transactions, impose conditions and mitigation measures, and recommend that the President of the United States block pending transactions or order divestures of completed transactions that raise such concerns. The Committee is chaired by the Secretary of the Treasury. To address identified national security risks, parties to a transaction can voluntarily file information with CFIUS to obtain clearance for the transaction to proceed or identify potential mitigation measures to allow the transaction to proceed. In certain circumstances, prescribed by regulations, filing with CFIUS is mandatory and failure to file may be subject to significant penalties – including fines up to the value of the underlying transaction.

2 The White House, "Background Press Call on President Biden's Executive Order on Screening Inbound Foreign Investments"

(14 September 2022), available at https://www.whitehouse.gov/briefing-room/press-briefings/2022/09/15/background-press-call-on-president-bidens-executive-order-on-screening-inbound-foreign-investments/.

3 Treasury Releases CFIUS Enforcement and Penalty Guidelines, U.S. Department of the (Oct. 20, 2022), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement-and-penalty-guidelines.

4 Treasury Releases CFIUS Enforcement and Penalty Guidelines, U.S. Department of the Treasury (Oct. 20, 2022), https://home.treasury.gov/news/press-releases/jy1037.

5 Section 1758 of the Export Control Reform Act of 2018 (ECRA) authorizes the Department of Commerce, Bureau of Industry Security to control the export, reexport, or transfer (in-country) of emerging and foundational technologies that are essential to the national security of the United States. ECRA was enacted as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019.

6 Committee on Foreign Investment in the United States Annual Report to Congress CY 2021, https://home.treasury.gov/system/files/206/CFIUS-Public-AnnualReporttoCongressCY2021.pdf

7 Department of Commerce, Bureau of Economic Analysis report re Direct Investment by Country and Industry (21 July 2022), available at https://www.bea.gov/news/2022/new-foreign-direct-investment-united-states-2021.

8 In 2020, CFIUS published a final rule that changed the rules defining "critical technology" transactions subject to mandatory filing requirements. It changes the circumstances where a "critical technology" investment will trigger a mandatory filing requirement by ending the use of North American Industry Classification System (NAICS) codes to identify specific industries subject to mandatory "critical technology" filings, in favor of a filing requirement based on U.S. export controls. In brief, a mandatory "critical technology" filing requirement is triggered under the final rule when a "U.S. regulatory authorization" would be required for the export, reexport, or transfer (in country) of the U.S. target company's goods or technologies to the foreign investor or certain other foreign persons involved in the transaction.

9 Foreign Investment Risk Review Modernization Act of 2018, Pub. L. 115-232, Title XVII, Subtitle A. (2018); 31 C.F.R. Parts 800 to 802. FIRRMA expanded CFIUS' authority to review certain transactions, joint ventures, minority stakes, and certain real estate purchases near military bases or other sensitive national security facilities.

10 The new law essentially codifies existing written and unwritten Bureau of Industry and Security (BIS) practices, policies, and definitions as they have evolved over the past 40 years, gives BIS enforcement officials more authority to investigate possible violations of the Export Administration Regulations (EAR), and directed BIS to identify "emerging" and "foundational" technologies warranting consideration for new export controls. The Act also creates a regular process by which BIS is obligated to continuously review, in conjunction with other agencies, emerging and foundational technologies that may need to be added to the Commerce Control List (CCL). The agencies charged with the responsibility of establishing new export controls include the Departments of Commerce, State, Energy, and Defense. Other agencies may provide support, as needed.

11 The White House, "FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China" (9 August 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/; U.S. House of Representatives, "CHIPS and Science Act of 2022," available at https://science.house.gov/imo/media/doc/the_chips_and_science_act.pdf. The CHIPS Act provides $52.7 billion in federal subsidies allocated to support chip manufacturing. Nearly three-quarters of the funding to be allocated over the next five years ($39 billion) is earmarked for the construction of semiconductor fabrication plants, or "fabs," including $2 billion specifically designated for mature semiconductors essential to the military as well as the automotive and manufacturing industries, including research and development and workforce cultivation.

12 These restrictions apply to any new facility unless the facility produces legacy semiconductors predominately for that country's market. Further, these restrictions – which would apply to funding recipients for 10 years from the date of funding – could shift. To make sure the restrictions remain current with the status of semiconductor technology and U.S. export control regulations, the law states that the Secretary of Commerce, in coordination with the Secretary of Defense and the Director of National Intelligence, would be required to regularly reconsider, with industry input, which technologies are subject to this prohibition.

13 Treasury Releases CFIUS Enforcement and Penalty Guidelines, U.S. Department of the (Oct. 20, 2022), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-enforcement-and-penalty-guidelines.

14 In contrast, The Department of the Treasury's Office of Foreign Assets Control's OFAC's Economic Sanctions Enforcement Guidelines are codified in its regulations. See 31 C.F.R. Part 501 (2022).

15 The Guidelines describe the types of conduct that can give rise to a violation under Section 721 of the Defense Production Act of 1950 and its implementing regulations, the process that CFIUS generally follows in imposing penalties, a non-exhaustive list of aggravating and mitigating factors that it may consider in determining whether to impose a penalty, and the scope of such a penalty. In brief, a party can violate the CFIUS regulations by (1) failing to make a mandatory filing; (2) failing to comply with a CFIUS mitigation agreement, condition, or order; or (3) making material misstatements or omitting material facts before CFIUS. Failure to file and mitigation-related violations are punishable by penalties of up to the greater of $250,000 per violation or the value of the transaction (with liquidated damages available if specified in a mitigation agreement), while material misstatements/omissions are punishable by penalties of up to $250,000 per violation.

16 Although CFIUS has had the authority to impose penalties since 2007, it has imposed only two penalties over time: 1) in 2018, the Committee imposed a $1 million penalty for repeated breaches of a mitigation agreement entered into in 2016, and 2) in 2019, the Committee imposed a $750,000 penalty for violations of an interim order. Additionally, in its most recent annual report, CFIUS noted it would continue to increase "staff resources dedicated to monitoring and enforcement activities."

17 See Section 721(f) of the Defense Production Act of 1950, 50 U.S.C. § 4565(f).

18 The White House, "Executive Order on America's Supply Chains" (24 February 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains.

19 The specific technologies identified in the CFIUS EO align with the most recent list of Critical and Emerging Technologies (CET) published by the U.S. National Science and Technology Council. See 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

20 Lauren Hirsch, David McCabe, Katie Benner, and Glenn Thrush, "TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain," New York Times (26 September 2022), available at https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html.