SOURCEREE

NATIONAL SECURITY NEWSLETTER

SEPTEMBER 2023

- CFIUS Review Standards: Incremental Risk, Totality of Risk, and Residual Risk
- FirstFT: Goldman Sachs Tapped Chinese State Money to Buy Western Companies
- US Probes Made-in-China Chip as Tensions Flare Over Technology

September 2023 Newsletter

National Security Investment Reviews

Issue 1: CFIUS Review Standards: Incremental Risk, Totality of Risk, and Residual Risk

Evaluating the Impact of Regulatory Boundary Conditions
Research by: John Lash, PhD

Issue: Promoting an open investment policy to attract foreign investment acts as a catalyst to strengthen the United States economy and conversely its national security. Investments, particularly those in high-risk high-reward technology industries, help to expand capabilities while providing necessary funding sources that may not be available domestically. National security reviews of foreign investments (conducted by the Committee on Foreign Investment in the United States, "CFIUS") are an essential component of protecting national security; however, with these reviews expanding in both frequency and scope, the concept of "national security creep" raises theoretical questions regarding the review process and has important practical implications for dealmaking and the economy.[1]

BLUF: **The standard for a national security review of a foreign investment follows statutory authority and should be objective, transparent, and fair in evaluating whether a particular transaction poses a genuine risk to national security. The procedural outcome of the review process must then represent a proportional response to the incremental risk (i.e., the threat, vulnerability, and consequence).**

〉 ***The Key Questions:***

- ***In Theory***: Does the statutory language for CFIUS reviews require that only the ***incremental risk arising from the transaction*** (i.e., the unique risk posed as a direct result of the deal) should be considered in the process?
  - *Consider: Legislative history, agency guidance, and public statements*
- ***In Practice***: Does CFIUS consider only the incremental risk arising from the transaction, or does the Committee evaluate the ***totality of the risk*** (including the risk that existed before the transaction which would exist without the transaction occurring)
- ***The Outcome:*** What is the impact of the application of an ***incremental risk standard*** (risk arising from the transaction) as compared to the application of a ***totality of risk standard which ensures there is no residual risk*** (even if such risk exists notwithstanding the transaction)
  - *Consider: Impact on national security, dealmaking, and an open investment policy*
- ***The Reality:*** Is it reasonable, or in the best interest of national security, for CFIUS to take a narrowly tailored approach to assessing risk in a transaction by only evaluating the incremental risk – and could these investments receive the necessary approvals if residual risk(s) went unaddressed because the risk did not directly arise from the transaction.
  - *Consider: CFIUS Congressional Reporting; Political Appointees leading agencies*

Reference Points:

- The language of CFIUS's statute suggests that Congress intended the Committee to conduct an ***incremental risk analysis*** of the threat ***directly arising*** from the covered transaction.
- **§ 800.102 Risk-based analysis.** Any determination of the Committee with respect to a covered transaction to suspend, refer to the President, or to negotiate, enter into or impose, or enforce any agreement or condition under section 721 shall be based on a risk-based analysis, conducted by the Committee, of the ***effects on the national security of the United States of the covered transaction***.

[1] https://columbialawreview.org/content/national-security-creep-in-corporate-transactions/

- FINSA states that "The Committee or a lead agency may, on behalf of the Committee, negotiate, enter into or impose, and enforce any agreement or condition with any party to the covered transaction in order to mitigate any threat to the national security of the United States that ***arises as a result of the covered transaction***."

Establishing a Connection from Pre-Existing Risk and Future Risk to "Incremental Risk": Practically speaking, the Committee can – and in some cases, must – attempt to establish a connection to risks which may not appear to directly arise from the transaction if those risks are reasonably believed to pose a detrimental impact to national security. CFIUS does not conclude action with respect to a transaction if "residual risk" exists – whether that risk is pre-existing, existing regardless of the transaction, or a prospective future-state risk.

〉 CFIUS will conclude all action with respect to a transaction if it determines that the transaction *does not pose any unresolved national security concerns*, that any national security concerns are *adequately addressed* by laws other than Section 721 and the IEEPA, or that *mitigation measures* agreed to or imposed by CFIUS *address any unresolved national security concerns*.[2]

〉 **Examples of Establishing Incremental Risk Connections:** At a basic level, something has changed about the composition of the company, its organization, and its management / control that has created "incremental risk" which may arise from the transaction.
  - ***Intent in the Threat Assessment***: In many cases, intent is triangulated by various inferences that are not necessarily technical in nature – they can be more geopolitical. Intent may be based on "home country / state interest" rather than individual interest of the individual investor. Even with existing risk of a company within a specific industry, the foreign investor creates a new threat vector that intensifies all of the existing and future risk.
  - ***Financial & Technical Capabilities***: But for the transaction, the company would not have had the financial capabilities to do "A," or to achieve "B," or to expand into "C." But for the transaction, the company would not have been able to hire the necessary expertise in a critical technology, obtain materials, establish key relationships, capture critical customers and corresponding Sensitive Personal Data.

Jurisdiction vs Risk: In determining the connection to national security risk arising from a transaction, CFIUS must ensure that it has both jurisdiction and a current risk to address. In some cases, this creates a paradigm where there was a legitimate national security interest in the transaction, but something has changed regarding the ownership structure or operations of the company wherein the "risk arising" is no longer current.

Jurisdiction vs Risk:

Jurisdiction can be had at any point in time on a Covered Transaction (for example, in a "non-notified transaction")

Example: An acquisition occurred in 2021 which was not notified to CFIUS but is a Covered Transaction – CFIUS has jurisdiction.

Risk must be current, as the risk addressed by CFIUS must be current.

Example: An acquisition occurred in 2021 but was sold / divested in Q1 2023; therefore, the risk arising from the transaction no longer exists – CFIUS has no current risk to address.

Therefore, there may be circumstances where CFIUS has jurisdiction, but the risk is not current, creating a transaction that CFIUS may not review.

[2] https://home.treasury.gov/news/press-releases/jy1663

Expert Perspectives: As part of the research process on these complex issues, experts in national security, cybersecurity, and technological innovation were interviewed, with key preliminary observations aggregated for further consideration. ***This line of inquiry established a focus on how CFIUS evaluates "incremental risk" as compared to "totality of risk" and the concept of "residual risk."***

Risk-Based Analysis for Foreign Direct Investment

- CFIUS reviews have to be incremental otherwise CFIUS is not reviewing the risk arising from the transaction (it's ostensible purpose) it is reviewing the vulnerability of a U.S. business that would exist even if the U.S. business were acquired by a U.S. company.
    - Evaluating the totality of risk (not incremental) creates threat agnostic results where CFIUS feels compelled to invent a threat where none exists so that it can plausibly (at least in terms of internal risk assessment) say that a risk "arises" (versus preexists) a transaction.
- The risk assessment should be based on the transaction before the Committee. Otherwise, parties do not have any real sense of how to address the risk of entering into a deal or the timeline considerations. It is also hard for parties to negotiate about how to assign the risk contractually.
    - If CFIUS intends to continue to utilize this broad-based risk assessment, it should provide more guidance on how it plays into the process.
- While the statutory language for CFIUS provides that only incremental risk arising from the transaction should be considered, the Committee does not practically operate in this manner. In fact, a Canadian acquisition may trigger mitigation if CFIUS believes that a third investment, where CFIUS does not have jurisdiction, needs to be mitigated.
    - In practice, this could be argued as operating outside of the authority of the Committee, and it could further impair national security because if and when the courts weigh in there could be a significant shift in how CFIUS reviews transactions that may restrict the broad – and at times necessary – latitude that the USG has for matters of national security.
    - That said, congressional acquiescence to nearly two decades of post-FINSA CFIUS practice would probably make the statutory language irrelevant from the perspective of an *ultra vires* lawsuit brought under the APA.
- CFIUS must be careful with establishing connections to theoretical risk, or along lines of "protectionist," "de-coupling," or "de-globalization" policies – such as imposing significant mitigation on U.S. companies with a global footprint *(making them less globally competitive with respect to supplier / vendor restrictions or restricting activities outside of the U.S.)*, or a U.S. company that has a business need to store data or intellectual property offshore *(for tax or other regulatory purposes)*, or which uses a globally dispersed workforce *(key software talent exists outside of the U.S. both in terms of capability and cost)*, or which has contracts with a Chinese entity for EAR99 products.
    - In practice, CFIUS reviews often slip into using jurisdiction as a mechanism to address preexisting risk, which is not the intent of the authority. *Why else would CFIUS be reviewing arguably greenfield transactions or borderline internal corporate reorganizations?*
- Generally, regardless of the language in the statute and regulations, many CFIUS personnel have expansive views of CFIUS authorities and, as a practical matter, CFIUS is not significantly constrained. This is partly attributable to (i) lack of judicial oversight / secrecy that shrouds CFIUS and (ii) the fragmented nature of decision making and related lack of responsibility. This represents a big and growing negative factor both from the perspectives of the economy and long-term security.
    - CFIUS should favor an incremental risk analysis, a high bar for finding risk before burdening transactions, and an obligation for an identified senior government official to articulate reasons for creating the burden.
    - For CFIUS, it is a much greater political risk to leave *any* national security risk unmitigated.
- CFIUS review has always meant incremental risk, and parties to a transaction generally approach CFIUS with this in mind, including an appetite for potential mitigation so long as it's incremental and not totality of risk.
    - Trying to assess totality as a baseline would likely break a transaction, as parties would (a) have no idea what to expect, and (b) trying to mitigate totality of risk could be a monumental task that could make the transaction no longer worth it.

    - Any founder starting a business in frontier tech, gov contracts, or anything that could have national security concerns would certainly pivot away from all of those buckets if they knew CFIUS was approaching risk in totality.
- The language that "only incremental risk arising from the transaction" could narrow the scope of the CFIUS review and could have a harmful impact on the quality of the risk reviews conducted by the Committee. The word "only" limits the ability of the committee to look broadly at the direct and indirect consequences of the transaction on national security.
- Due to evaluating the totality of the risk, including risk that exists regardless of the transaction, CFIUS has created a default presumption of the transaction parties without assessing the parameters of a specific transaction.
    - The Committee is generally shielded from supporting risk assessments as there is limited information provided about the factors of the risk calculus.
    - The downside of hiding the ball is that the best deal for the benefit of the US business may not always be pursued because of the perceived uncertainty of what CFIUS's mandate may be. There is a tension between business and national security interests and that is only growing because the Committee is increasingly overstepping outside the parameters of a transaction.
- CFIUS is heavily incentivized to focus on relatively remote risk – which includes expanding the review towards pre-existing risk and theoretical future risk.
    - This is ironic considering that the U.S. has derived significant strength in national security benefits from drawing capital inward.
- The statutory language speaks to both reviews and investigations evaluating risks arising from the transaction, which should be interpreted to mean incremental risks. But if the transaction in front of CFIUS, building upon previous ownership interests, gives the investor rights it didn't have before, then it is still an assessment of the cumulative investment *(defining cumulative as inclusive of incremental)*.
    - CFIUS never considered (and to my knowledge, does not consider) "totality of risk," since a parallel risk can arise from multiple sources outside the scope of the transaction in front of it.
- The Executive Order (14083) giving guidance to CFIUS makes the incremental risk assessment moot. Now CFIUS is directed to consider aggregate risks, or the risks of one transaction when viewed in the context of other transactions.
    - However, this approach, which is contrary to the approach historically used by CFIUS, is unfair and arguably unenforceable without a more transparent process.

Issue 2: FirstFT: Goldman Sachs tapped Chinese state money to buy western companies

Source: https://www.irishtimes.com/business/2023/08/29/goldman-sachs-bought-uk-and-us-companies-using-chinese-state-funds/

Considerations:

- Goldman Sachs established a fund using Chinese government money to acquire American and British-based companies, including one engaged in cyber security services for the U.K. government, the Financial Times reported.
    - Goldman used cash from the fund to buy seven companies, including LRQA, whose subsidiary, Nettitude, is a cyber security firm that provides services to the British government.
        - The business includes cybersecurity group Nettitude, which says on its website that it is an approved service provider for the UK government and helps to "strengthen government and defence organisations across the world". Its work includes "ethical hacking", in which its staff attempt to hack clients' systems to assess their vulnerabilities.
    - A spokesperson for LQRA, which carries out inspection and certification services for the British military as well as energy and health care sectors, told FT: "China represents 40% of the global certification market and we are currently under-represented there, which is something we are seeking to address in part with assistance from the [Goldman-CIC] fund."
    - Goldman also used funds from the CIC to acquire Project44, a tech startup that tracks global supply chains; Cprime, a cloud-computing consultancy firm; Parexel, a drug-testing company; and Boyd Corporation, a manufacturer of AI and drone systems, according to FT.
- Despite increasing tensions between Beijing and Western nations, Goldman has inked seven transactions through a $2.5 billion private equity "partnership fund" it created with China Investment Corporation (CIC) in 2017, according to numerous individuals who possess firsthand insight into the fund and its operations and who spoke to the FT.
- These transactions encompass a range of sectors, including global supply chain tracking, cloud computing, drug testing, manufacturing systems for AI, drones and electric vehicle batteries, according to the FT.
- The fund's partner, CIC, said it would serve as an "anchor investor" with active involvement in helping to expand the acquired firms in China. CIC is a sovereign wealth fund controlled by Chinese state.
- Goldman said in a statement to the FT that "the co-operation fund is a US fund run by a US manager, and is managed to be in compliance with all laws and regulations. The bank added that it "continues to invest in U.S. and global companies, helping them increase their sales into the China market."

Issue 3: US Probes Made-in-China Chip as Tensions Flare Over Technology

Source: https://www.reuters.com/technology/huaweis-new-smartphone-uses-more-china-made-parts-than-previous-models-2023-09-07/

Considerations:

Highlights

- The Biden administration's efforts to limit China's access to high-tech semiconductor chips and advanced machinery for supercomputing and AI have yet to be successful. There is growing frustration in Washington this week after Bloomberg revealed that Huawei Technologies Co. and China's top chipmaker, built a new smartphone using an advanced 7-nanometer processor.
    - For some context, Apple's current iPhones use 4nm chips. The introduction of new iPhone 15 models will likely be powered by 3nm next week. Even though there is a sizeable gap between Huawei's 7nm powered smartphone and Apple's 4nm, it demonstrates the possibility that sanctions have been an ineffective weapon by Washington against China.
- On Tuesday, US National Security Adviser Jake Sullivan told reporters he needs "more information" on the "character and composition" of Semiconductor Manufacturing International Corp.'s Kirin 9000s chip powering Huawei's Mate 60 Pro. Financial Times reported Sullivan was responding to a question during a briefing when a reporter asked whether US controls on exports of advanced semiconductors were being circumvented by Beijing.
- TechInsights conducted a complete teardown of the Mate 60 Pro for Bloomberg. They found that the "processor is the first to utilize SMIC's most advanced 7nm technology and suggests the Chinese government is making some headway in attempts to build a domestic chip ecosystem."
- Huawei Technologies' new high-end smartphone contains more China-made chip components than previous models in a sign of Beijing's advances in the semiconductor sphere, according to research firm TechInsights, which is taking the device apart.
- "It looks like more than half, maybe two-thirds of the silicon is domestically grown capability, where in the phones we were seeing 2-3 years ago, a third was domestic. That's another really big advance they've made," Dan Hutcheson, an analyst with TechInsights, told Reuters.
- "The significance is that it shows that China has been able to stay 2-2.5 nodes behind the world's best (chip) companies. People thought they would be stopped at 14 nanometer," Hutcheson said.
- Some research firms forecast SMIC's 7 nm process has a yield rate below 50%, versus the industry norm of 90% or more, and the low yield would limit shipments to around 2-4 million chips, not enough for Huawei to regain its former smartphone market dominance.
- Some early users of the phone have also posted videos of the phone containing NAND flash memory chips made by South Korea's SK Hynix Inc (000660.KS), which voluntarily suspended chip sales to Huawei after the Chinese firm was hit by Washington's sanctions.
- "SK Hynix no longer does business with Huawei since the introduction of the U.S. restrictions against the company and with regard to the issue we started an investigation to find out more details," the company said in a statement. “SK Hynix is strictly abiding by the U.S. government's export restrictions."