Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How The CFIUS Calculus Continues To Change

By **Stephen Heifetz and Joshua Gruenspecht** (March 1, 2018, 12:35 PM EST)

Stephen Heifetz

Joshua Gruenspecht

A recent focus on outcomes produced by the Committee on Foreign Investment in the United States — particularly CFIUS scuttling far more deals than ever before — has obscured a shift in principles that seemingly underlies the new approach. The change in administrations is an important factor contributing to different outcomes, but CFIUS — the government committee that conducts national security reviews of foreign investments in U.S. companies — remains an analytical body that justifies its decisions, at least internally, by reference to principles.

For many years, CFIUS has been guided by the concept of the "risk delta" — i.e., that the increase in risk that may result from a transaction determines what CFIUS action is warranted. However, the risk delta analysis is only loosely tethered to law, so it is subject to change or elimination. And it appears the concept has evolved substantially in the last year — a change to the CFIUS calculus that may alter the types of arguments that resonate with CFIUS.

Risk Delta: Lore, Not Law

The law governing CFIUS states that the committee may seek to mitigate any risk that "arises as a result" of a transaction over which CFIUS has jurisdiction. CFIUS agencies historically have agreed that this means the committee's actions should aim at any potential increase in risk over the status quo. That is, CFIUS should take adverse action — imposing conditions ("mitigation measures") or refusing to clear the deal — only to reduce or eliminate any significant risk delta arising from a specific transaction. While this principle is based on the "arises as a result" language, it is not clearly prescribed by that language. Like many features of CFIUS, the risk delta principle is more a matter of lore than law.

Measuring the risk delta is distinct from assessing whether a transaction presents risk. To see this point concretely, let's suppose an Israeli company forms a U.S. cybersecurity company — San Jose-Israeli Cyber, or SJC — which wins some contracts with local law enforcement.

Now suppose that a German company signs a deal to acquire SJC from the Israeli parent. CFIUS accordingly would delve into the details of the potential German acquirer — the company's compliance with applicable laws, who owns and manages the company, and whether those individuals have ties to anyone of concern to the U.S. government, such as hackers, terrorists or adversary governments.

Let's imagine that CFIUS found little or no adverse information about the potential German acquirer. At the same time, CFIUS might note possible concerns about SJC's current Israeli parent: while Israel and the United States have been close allies in many regards, the two countries' spy agencies are known to work against each other at times**.**

Accordingly, CFIUS might conclude that while there would be national security risk associated with a German company owning SJC — presumably it would be better to have SJC owned by Americans — nevertheless the risk delta is minimal or zero. That is, the transfer of ownership to a German company from an Israeli company does not create a material increase in risk over the status quo.

In light of the absence of any risk delta, CFIUS might conclude that it should clear the transaction without any conditions. Since mitigation measures historically have aimed to reduce or eliminate the risk delta, if there is no material increase in risk, then there should be no risk mitigation measures.

The Value of Data

When we consider a more common scenario, though, it is apparent that the risk delta concept has changed. Suppose a Chinese state-owned company plans to acquire the hypothetical mid-Atlantic regional realtor, USHOMES. USHOMES has a growing database of 10-plus million homes and the names of individual residents, along with ages and genders culled from publicly available data. That same data exists in several other databases and is available for purchase, but to get the exact same dataset held by USHOMES, one would have to purchase data from multiple alternative databases.

If recent history is a guide, there is a reasonable chance that CFIUS would scuttle a Chinese acquisition of USHOMES. Why? Because of concerns that the data could be used for espionage purposes — the U.S. Department of Justiceand the U.S. intelligence community, in particular, are concerned that Chinese acquisition of U.S. citizen information facilitates spying on those citizens, some of whom may hold positions in government or the private sector that are relevant to national security.

The parties might argue that the Chinese government does not need to acquire USHOMES data for espionage purposes — it can purchase the same data from alternative databases. Some CFIUS officials would reply, however, that easy access to USHOMES data would nevertheless facilitate espionage, or that the USHOMES data might include data points not available elsewhere.

Does a Chinese acquisition of USHOMES present an increase in espionage risk? Yes, in the sense that even an iota of data arguably increases that risk. But this seems to stretch the notion of the risk delta, as the delta is so miniscule as to be functionally zero.

A Zero-Sum Competition?

However, viewed against the backdrop of U.S.-China relations, at least as understood from the perspective of many national security officials, it is not surprising that the risk delta concept has changed, at least for deals involving strategic competitors like China.

Through both Republican and Democratic administrations, many national security officials have held a "zero-sum" view of the U.S.-China relationship. Schooled in a mainstream understanding of international affairs as a competition between great powers, these national security officials maintain that virtually any China gain is a U.S. loss. If a Chinese company seeks to acquire a U.S. company, that fact by itself is reason to oppose the deal — at least if any plausible argument can be made that the U.S. company could be used to harm U.S. security.

This zero-sum view exponentially increases any risk delta: If the question concerns a zero-sum competition among great powers, the U.S. and China, then even a negligible risk delta — perhaps an iota of data about U.S. persons that could be obtained from a U.S. company — likely will be viewed as a major security problem.

Further, because any data acquired in one transaction could be aggregated with data acquired in other transactions — and if one views a transaction through the prism of a zero-sum great power competition, then aggregation would be assumed — an iota of data may become a critical component of a larger database. USHOMES has a small amount of data that might be helpful for espionage purposes? The answer is easy: oppose that deal.

While the zero-sum position has had proponents for years, it generally has not been supported by agencies that focus on economics and trade matters, such as the U.S. Department of Commerce or the Office of the United States Trade Representative. These agencies have tended to view international trade and investment as "win-win," and in the past administrations have countered or softened the zero-sum view when it has been advanced by the security agencies.

In the current administration, however, the trade-focused agencies have developed a pronounced skepticism about the benefits of international trade, in particular between the U.S. and China. Meanwhile, the views of the national security agencies, such as the departments of Justice and Defense, are on average more hawkish than before. The zero-sum view is ascendant both among the national security agencies and, in many cases, within the trade agencies.

The Consequences and a Path Forward

The predominance of the zero-sum view means that even negligible risk deltas might be unacceptable to CFIUS when the acquiring company is from China (or Russia). That is particularly so if the transaction enables the acquirer to obtain data or other assets that can be aggregated through multiple transactions. Arguing that the risk delta is negligible, while a plausible strategy in previous administrations, might not facilitate CFIUS clearance today.

That does not mean, however, that such deals cannot be cleared. Whereas the risk delta principle historically served to focus CFIUS narrowly on the risk arising from a particular transaction, the current broadened analysis presents a corresponding benefit, if CFIUS applies its new principles consistently — i.e., taking a broader view of international relationships enables consideration of other context that might weigh in favor of clearing a deal.

For example, there are some situations when a business that supplies important products or services to national security agencies might fail if CFIUS does not clear a foreign investment. That is not risk arising from the transaction, but it is context relevant to assessing risk.

Similarly, risks inherent in a U.S. business could be addressed via a CFIUS mitigation agreement. USHOMES, for example, could sell its data to a Chinese company, and the sale of that data would not be subject to CFIUS review. But in a CFIUS-reviewed transaction to acquire USHOMES, the buyer could enter into a mitigation agreement with CFIUS in which the parties agree to limit data access to U.S. citizens. In that way, the transaction could improve the U.S. security posture — data that would have been available for sale to anyone would become restricted.

Several senior CFIUS officials have indeed espoused the view that CFIUS should consider not only the potential consequences of clearing a transaction, but also the negative effects of failing to do so (including collapsed businesses) and the potential positive impact of mitigation agreements. Mitigation agreements that improve national security in comparison to the status quo, such as the restriction on providing USHOMES data, would seem to advance not only U.S. national security but also U.S. economic interests as articulated by the Trump administration: Just a few weeks ago, the Trump White House **endorsed** the "twin aims of protecting national security and preserving long-standing United States open investment policy."

Why have we not seen more mitigation agreements in recent China deals? Some CFIUS officials have argued that compliance with such agreements cannot be assured, or that the agreements are too expensive to implement. But such categorical dismissal of mitigation agreements seems to cut against the prevalent contextual analysis. There are myriad ways of handling compliance concerns, including the use of independent monitors paid for by the deal parties, with severe penalties for breaches. Is there risk of breach? Perhaps, but that risk may be far less than the risks that ensue from quashing the deal and letting USHOMES data flow freely.

CFIUS is well-aware of this, of course. And as the risk delta principle continues to morph into a zero-sum, contextualized analysis, at least for deals involving China and other strategic competitors, we might see the resistance to mitigation agreements fade. Arguments that CFIUS can improve national security by clearing a case with a mitigation agreement might, in time, have greater resonance.

Stephen Heifetz is a partner and Joshua Gruenspecht is of counsel at Wilson Sonsini Goodrich & Rosati

PC in Washington, D.C. Heifetz previously served on the Committee on Foreign Investment in the United States.