JULY 11, 2022

Exploring the costs associated with CFIUS mitigation and compliance

This week, we sit down with Steve Klemencic, managing director at global consulting firm BRG. A former senior analyst at the National Intelligence Council where he focused on CFIUS matters, Klemencic previously served as division chief at the Defense Intelligence Agency providing intelligence support to the DoD as a voting member of the Committee. He also helped stand up the National Intelligence Council's CFIUS Support Group and the FBI's Foreign Investment Unit. Currently the CFIUS leader at BRG, Klemencic has served as a U.S. government-approved CFIUS compliance monitor or auditor at several companies..

Steve, let's talk money. We've written a ton about mitigation agreements, from what the DoJ considers an effective agreement, to corporate considerations and even examples of National Security Agreements. But we haven't talk about costs associated with these agreements. So, stupid question first: Are costs an issue?

Ah yes, everyone's favorite topic ... cost! The short answer is, yes, costs can be an issue, but are not always. A lot depends on the regulatory compliance ecosystem inside the company and level of difficulty required in installing NSA mitigation measures. There is a wide range of costs associated with implementation, from enhanced physical and cyber security measures to increased privacy and data protection measures.

But there are other factors as well. What is the asset being protected? Is it a technology, a process, intellectual property, or some form of personal data? Who is the foreign investor and what are the related concerns? How sophisticated is the company in terms

of regulatory compliance? What changes will need to be implemented to reorient or strengthen compliance programs? How large is the company? How expansive is the mitigation? Is a third-party monitor or third-party audit required? How involved will the third-party providers have to be? At the risk of sounding very lawyerly, the best answer really is, "It depends."

Makes sense. But, in your experience, what are the largest categories of costs associated with mitigation agreements?

There is a lot of attention being paid to privacy and data protection, and often companies do not do that as well as they think they do, so enhancements may be required. How well, or not, relevant intellectual property is protected can be a factor. In a couple of particularly complex cases that I'm familiar with, U.S. customer data held by the U.S. target company had to be moved to a U.S. location and held by a U.S. government-approved and U.S.-owned third-party repository. As you can imagine the cost for storing the data and controlling access to the data on behalf of the target company can be significant to business operations.

In a completely different context, physical security usually is not much of an added cost unless the U.S. target company has only very basic techniques in place — think lock and key— and have never really considered measures beyond that, have only the most basic corporate security infrastructure in place, and suddenly find themselves classified in a CFIUS transaction as critical infrastructure and located within proximity to sensitive U.S. government installations. In that case, a complete buildout of physical security measures is required which then becomes a cost driver.

So it sounds like the major costs are closely tied to implementation plans?

Absolutely. In a general sense, you can put costs into two buckets. The first is mitigation implementation, which covers upgrades to or installation of systems used for privacy and data protection and cybersecurity, physical security, adjustments to business operations, and whatever else is required to put the mitigation measures in place. The second is mitigation compliance, which includes third-party monitoring and third-party auditing.

What are some unanticipated costs?

I think it's fair question, but due to the differences in mitigation agreements between companies, I think it's better to consider why you have unanticipated costs. The majority of the unanticipated costs I've seen have resulted from one of three sources.

First, the deals teams that negotiate the transactions do not always communicate well with the corporate leadership of their client the terms to which they are agreeing to attain U.S. government approval of the transaction. This results in poorly thought-out mitigation implementation plans and unanticipated implementation costs. It has become important for CFIUS counsel to press the deals team to ensure that corporate leaders are fully aware of, and understand the implications of, what is being agreed to and why.

Second, and not to place all the blame on the deals teams, there are times corporate leadership simply does not fully understand the requirements and complexity of the mitigation agreements, which also results in poorly thought-out implementation plans and unanticipated costs. The keys to avoid problems are: 1) Effective communication between deals teams, CFIUS counsel, and corporate leadership; and 2) Establishing a collaborative relationship with the CMAs [CFIUS Monitoring Agencies] in which to work through issues as they arise.

The third source of unanticipated costs is a breach of compliance with the NSA resulting in an investigation. Whether intentional or accidental, the investigations cannot be anticipated and unfortunately can be costly.

So, based on that, in your experience, have companies done a decent job preparing for these costs, or are most caught off guard with the complexity of the mitigation agreements and compliance requirements?

For the most part, yes, companies do a good job preparing for these costs. They really do want and try to do the right thing and work very hard to make sure the implementation of the mitigation agreement is well planned, executed, and funded. There are occasional exceptions to this, of course, which can result in a lot of anxiety, but I haven't seen an issue yet that could not be resolved somehow.

In an interesting sidenote, one of the areas where companies often act aggressively to contain costs is with mitigation compliance requirements such as third-party monitors and third-party auditors. Given the cost of implementation, in many cases there is real pressure on third-party compliance providers to keep fees down when competing for the work in order to minimize additional costs.

Have you found CFIUS to be sensitive to some of these costs? Or not so much?

Contrary to the belief of many companies going through CFIUS mitigation negotiations and implementation, CFIUS is cognizant of the additional implementation costs that may arise and the potential impact of mitigation measures on business operations. The key is communicating with the CMAs. It's been my experience that CFIUS does appreciate the cost and impact of these agreements and will often work with companies concerned with controlling such costs and impacts. The CFIUS reps at the ACI conference back in April very readily admitted they do not know everything about everything, and if you have a more efficient and cost-effective means to accomplish the same goal, they will consider your suggestion or request.

What is critical to understand, though, is that at the end of the day CFIUS will not abrogate its responsibility to protect U.S. national security simply because a mitigation agreement is expensive or difficult to implement.

Is there a way that companies can calculate or account for the costs of mitigation?

How individual companies calculate the costs of mitigation really is up to them. At the most basic level, though, the common denominator through it all is effective communications between the deals team, corporate leadership, and the teams that will be responsible for implementing and operationalizing the mitigation agreement. There must be a clear understanding across the board of what is being negotiated and agreed to and its impact on cost and business operations.

Are there any "best practices" to employ, or — perhaps more helpful to our readers — "worst practices" to avoid?

Here are some things to think about:

- Make sure to include the people responsible for mitigation implementation in the discussion about mitigation measures. They are the people who will have to make the measures work, and will likely have the best insight on practicality, schedule, and cost.
- Do not agree to mitigation measures with the Committee unless or until you fully understand the implications of what you are signing up for. That means there must be effective communication not only within the company and its advisors, but also between the company and CFIUS.
- Do not try to change the National Security Agreement after it has been executed. CFIUS is not going to renegotiate.
- Do not be afraid to engage with the CMAs to work through implementation issues. They do not have all of the answers and are willing to listen to suggestions and recommendations on what may be a more effective or efficient method to

implement a particular measure than that originally stated in the NSA.

Any other thoughts or recommendations for companies?

In no particular order of importance:

- Keep apprised of the evolving geopolitical environment and how it might impact your transaction. It may help you understand why CFIUS makes some of the mitigation decisions it does.
- Remember you are dealing with people charged with protecting U.S. national security, and they will apply that writ broadly. You might not like it, but frankly it is their call to make.
- There will be information the government holds that may impact mitigation that it simply cannot tell you about. It can be frustrating, but they legally cannot tell you.
- Be prepared in case something bad like a breach happens. How will you react and respond? It's better if you have a plan in place so you can better control the fallout.
- Finally, communicate and collaborate internally, and communicate and collaborate externally with CFIUS and the CMAs. Everyone has a job to do, sometimes those jobs run counter to each other, but everyone is trying to do the right thing.

Thanks Steve.

Steve Klemencic is Managing Director at BRG. He can be reached at sklemencic@thinkbrg.com or (571) 334-4602.