TUESDAY, AUGUST 19, 2020

CFIUS risk assessments, audits, and mitigation agreements

EisnerAmper partner Michael Rose.

This week, we speak (virtually, of course) with Michael P. Rose, a partner at EisnerAmper who serves as the firm's National Practice Leader for CFIUS Advisory Services. We explore the components of a pre-filing risk assessment, pitfalls for companies to avoid, controls and procedures to ensure compliance with mitigation agreements, third-party compliance audits, and more.

Michael, let's start by talking about risk assessments for transactions, pre-CFIUS filing. In your experience, what should a risk assessment include?

The first step in the risk assessment is: Know who the owners are really going to be. A risk assessment is an examination of what could cause harm or delay the closing of a transaction. The assessment should consider both the acquiring/investing party and the target [U.S.] company. Knowing the potential obstacles one might encounter before entering into a transaction can help in assessing whether or not to go forward.

Some of the first items to review are:

1. Are we a covered transaction?
2. Has foreign ownership been verified?
3. What is the risk tolerance of not filing with CFIUS?
4. Are there other ways to structure the deal such as convertible debt, with no control rights, or a bridge loan, to avoid a filing or jurisdiction under CFIUS?

Consider the potential positive impact of self-mitigation early in the deal cycle, when the company still has a fair amount of control over the variables.

What about specifics for the foreign acquiring or investing company?

As an acquirer, consider your country of domicile along with any known government contacts and contracts. You must also look into ties to other foreign countries — through business ventures, subsidiaries or government contracts — that may be of higher risk than your own domicile. The reason for the acquisition

should be clearly documented including how it fits into the organization. As part of the purchase/investment, it is incumbent on the buyer to know what the effort and costs might be to satisfy U.S. regulators.

And for the U.S.-based entity?

As the target or selling party, you should have clear policies and procedures over critical technology, critical infrastructure and customer data (TID Business) if they exist. Supply chain, business lines and locations, sales channels, IT architecture and vendor management programs are also considered in the evaluation. Additionally, any existing government contracts should be reviewed. If you own real estate and it is utilized or leased, the proximity to U.S. government facilities should be evaluated as well as determining what, if any, government tenants are present as both may need to be addressed.

Understanding CFIUS concerns up front with regard to a potential acquisition is critical. The pre-filing risk assessment should include the following:

- Vulnerabilities/risk of U.S. target to national security
- Foreign threat capability
- Consequences if vulnerability is exploited
- Foreign government controlled transactions
- Transfer of sensitive technologies
- Proximity of U.S. target facilities
- Sensitive personal data
- Critical infrastructure
- Supply chain security

Are there specific things you've seen in your practice to date?

Some of the concerns that we have seen include:

- Foreign intelligence collection; proximity to sensitive facilities, sensitive technologies and personal data access
- Foreign military/intelligence capabilities; military technologies, emerging technology
- Domestic needs; continuity of supply to the government and critical natural resources
- Critical infrastructure; supply chain security and product integrity

Are there any lessons you can impart to companies or investors about this process? Any pitfalls to avoid?

At the onset of the transaction, or when just contemplating investments in the U.S, investors should consider whether the deal has any potential U.S. national security implications and, if so, what that could mean in terms of additional costs and time to close a transaction. It is also important to know that even non-controlling foreign investments or interests in TID Businesses could cause CFIUS concerns and actions.

Mitigation measures should be discussed by both parties so that information can be provided to CFIUS in the beginning and before they mandate certain requirements. If CFIUS could impact the transaction because the U.S. company is a TID Business, consideration should be given for a voluntary filing. Also, as part of the pre-filing risk assessment, preparation should be made for discussions with CFIUS in addition to consideration given to factors that would be involved if a mandatory mitigation agreement is required. This upfront planning will assist in the discussions and knowledge of what is achievable if a mitigation agreement is required.

As CFIUS has the authority to cause a transaction to be unwound years after it was closed, consideration to make a voluntary filing in order to obtain a "safe harbor" ruling should also be considered.

If the parties fail to make a mandatory filing, CFIUS could impose significant

monetary penalties which could include the unwinding of the deal itself.

John Demers at the DoJ has been outspoken about the use of mitigation agreements. He's noted that internal compliance controls and procedures are critical to effectively monitor and ensure compliance. What policies, controls and procedures have you seen companies employ?

Where a mitigation agreement was put in place, specific policies and procedures have been established to ensure compliance. In addition to the policies and procedures, controls have been established to ensure that the contract compliance is adhered to in the mitigation agreement. Also, a review is recommended in the first year to determine that the policy and procedures are effective. Some examples of focus areas include:

- Creation of Security Director and Security Officer Positions along with documented roles and responsibilities.
- Cyber policies and practices along have been expanded to include continuous monitoring of control activities along with escalation protocols.
- Restriction of access to facilities.
- Existing practices such as application/system access may require additional approvals and stringent monitoring of "protected" data.
- Training of Management, Staff and Board Members on the mitigation agreement and their roles with respect to it are essential.
- Very tight governance procedures around the securing of company information and access to that information.

Is there anything you specifically recommend when it comes to policies and procedures, whether it be training, communication, or security?

It is all of the above. It is important to understand what is presently in place, how the policies are built with respect to the mitigation, and whether the company can incorporate mitigation terms into existing policies or if new policies need to be written. We suggest implementing policies and procedures around the articles in the mitigation agreement and controls to ensure that the policies and procedures remain in effect.

Communication is key with a delegation of roles and responsibilities. Training, training and more training. Everyone involved with the areas addressed in the mitigation agreement must know their responsibilities and that includes communication to and from the legal teams and the Security Officer and Security Director. It is also important that the all parties communicate with each other to ensure that items do not fall between the cracks, leaving both parties vulnerable. We also suggest doing an annual review of those controls around contract compliance focusing on the original design and operating effectiveness.

Since sharing of information that could have national security implication is of course not allowed, both physical and logical access to property, systems and e-mail communications must be monitored at all times

What about compliance audits? Is that something you've seen or are recommending?

Yes, we have been working with companies to help them comply with mitigation measures by assisting them with designing appropriate controls and evidence to support that the controls are operating effectively, known as readiness. We have also executed some of these third-party

compliance audits. Typically, if a company is undergoing a third-party compliance audit, it is because it is required by their national security agreement. Most commonly it is stipulated that the audit be completed by a third party, and that third party is subject to approval by the CFIUS monitoring agencies, known as the CMAs, which is comprised of the Department of Treasury and the Department of Justice among other agencies. We have recommended that companies go through a mock audit to prepare themselves for the actual audit.

The CMAs are empowered to monitor and enforce mitigation agreements. Compliance audits are a tool by which CFIUS is able to monitor if the transaction parties are adhering to their national security agreement.

Are you seeing CFIUS-related activity in the real estate market?

As Foreign Investment Watch I know has covered, the real-estate provisions of FIRRMA are fairly recent in the evolving progression of CFIUS regulation. CFIUS always had the review power if real estate as part of an overall transaction had a national security concern. However, under the new legislation and regulations, CFIUS has jurisdiction if a real estate transaction meets certain criterial relating to military installations, maritime ports and certain other specific areas. In addition, if the acquisition of real estate may involve critical infrastructure, critical technology or sensitive customer data housed in the real estate, this may be also looked at. There are certain exceptions in the regulations.

Any specific examples you've seen?

EisnerAmper has a new client which is a boutique investment and advisory firm that focuses on infrastructure and real estate. They also provide advisory services to assist in transaction execution. The company has assisted a foreign investor in a number of real estate deals in the U.S. in the form of acquiring interests in buildings and complexes where the U.S. Advisor may or may not take an investment interest. Until now the deals have been for apartments or condos in large cities across the U.S. Unbeknownst to the advisory firm, the past real estate deals have fallen under exceptions to the CFIUS regulations as we will discuss later.

The next deal is for an office complex in a major city. This deal could be covered under the regulations as although it might not fall directly under the exact criteria under 31 C.F.R. Part 802, it will incorporate national security concerns around critical infrastructure and can be considered critical. The office complex will house one of the largest energy infrastructure, fiber optics and telecommunications companies in the U.S. There will be much risk with this transaction and an assessment will be needed to be completed to determine if a voluntary filing is required. Where foreign investment in the U.S. takes place in real estate transactions, one must look to the Section 802 regulations but must also assess if the transaction could be considered a national security risk around critical technology or critical infrastructure.

Any recommendations for companies related to this?

While the Treasury Department has whittled down some of the final regulations from the initial proposals, there is still potential for unpleasant surprises for real estate under 31 C.F.R. Part 802, the 31 pages of final rules governing real estate transactions under FIRRMA. Filing with CFIUS for "covered" real estate transactions are voluntary. As it is not a mandatory filing requirement but the CFIUS considerations should absolutely be part of the purchase or lease checklist. However, obtaining pre-clearance provides the parties to the transaction with a regulatory safe harbor

which would prevent CFIUS from later suspending the transaction for national security reasons. The following five areas should be considered.

- A foreign company doesn't need to acquire a U.S. company to be covered by the new rules for CFIUS review of a real estate transaction.
- CFIUS can only review deals that give investors three of the four property rights.
- The Treasury Department is providing investors with definitions around close proximity and extended coverage.
- There are fairly broad exceptions under the new rules for single-family, housing units and commercial office space.
- The D.C. metro area and other parts of the country with dense concentrations of government and military facilities may be more affected by the new real estate rules despite the exceptions for "urban clusters" and "urbanized areas" in the regulations.

MORE INFORMATION

Michael Rose is a Partner at EisnerAmper specializing in Process, Risk, and Technology Solutions. He serves as National Practice Leader for the firm's CFIUS Advisory Services. With over 35 years of consulting, technology and audit experience Mike's focus is internal audit, internal control, governance and risk management, utilizing digital strategies to improve performance. He can be reached at (215) 881-8168.