Guidepost

WHEN TO CONSIDER CFIUS MITIGATION REQUIREMENTS? NOW!

As my colleague Ken Mendelson noted, the watchword for ACI's recent CFIUS conference was "mitigation." As a result of the new rules implementing the Foreign Investment Risk Review Modernization Act ("FIRRMA"), the number of deals requiring mitigation is likely to grow significantly.

The conference, however, focused mostly on the kinds of deals that would require mitigation. The conference offered little detail regarding the specific mitigation measures that might be sufficient to get a transaction approved. Those measures could be a critical factor in securing approval.

A company that fails to consider mitigation measures early could find out very late in the game that either the game is not worth the candle – mitigation is just too onerous – or that CFIUS will not approve the deal because the structure and purpose of the deal forecloses adequate mitigation measures. While each deal is unique, and the mitigation CFIUS requires will be tailored to the risks a deal poses, in our experience working with entities facing CFIUS issues, there are several mitigation steps that appear to be helpful when mitigation is required.

First, implementation of any mitigation measures is likely to require the target entity to designate a security officer, usually a US citizen and senior company official. The security officer will be responsible for ensuring, and fully documenting, that the CFIUS mitigation measures taken by the target entity are adequate to protect the national security interests of the United States. These mitigation requirements are typically spelled out in either a national security agreement ("NSA") or a letter of assurance ("LOA") depending on which one is chosen by the transaction parties and CFIUS. For many measures required by an NSA or LOA, the security officer will be the official responsible for receiving reports, reviewing the effectiveness of the measures, and certifying to and reporting on compliance to the government.

The security officer will need substantial support to perform these duties while still performing his or her day job. Such support is common in bigger companies that have a chief compliance officer and a general counsel's office. Smaller companies may need to hire the infrastructure to develop policies and procedures and assist the security officer in overseeing compliance.

Mitigation could also involve the governance of the acquired entity. In some cases, the government will insist that the acquiring firm be treated like a passive investor for the purposes of governance. This can be effectuated by interposing a board of voting trustees generally made up of U.S. citizens with a national security background, who independently serve as a *de facto* Board of Directors, making high level decisions like approving business strategies and overseeing executive responsibilities.

This will not mean that the acquiring company cannot work with the acquired company on those matters. It just means that ultimate decisions belong to the trustees, who are required to act independently to protect the national security interests of the United States, consistent with their general corporate fiduciary obligation.

Acquisitions of companies with sensitive technologies may require mitigation measures that protect that technology from access by foreign entities, especially the acquiring company and its personnel. Such measures might include storage of formulas, software details, or other intellectual property (IP) in secure facilities or on secure servers, implementing robust access controls and a cybersecurity program that include appropriate monitoring of systems for attacks and other unauthorized access, limiting physical or online access to those who have a need to know, maintaining logs of all access attempts, and developing an insider threat assessment program. The target entity should also ensure that vendors to whom sensitive IP is transferred for use in manufacturing components or products are able to meet physical, technical, and administrative security standards and can certify they have done so.

In some cases, the acquiring company's interest in the target entity may involve sales of the target's products to and through the acquiring company. In addition to the protections noted above regarding the physical security of the target's networks and its sensitive IP (i.e., through encryption) communications regarding sales and marketing to and through the acquiring firm may also have to be monitored and/or restricted to prevent disclosure of the IP to the personnel of the acquiring company.

Mitigating the possibility of inadvertent or intentional disclosure of sensitive IP either through the development of business strategies or plans or through sales and marketing efforts can be accomplished by carefully controlling and documenting who is allowed to communicate regarding those matters with the acquiring company, and what information can and cannot be shared. In the case of business plans and strategies, only senior company officials might be allowed to discuss them. In the case of sales and marketing efforts to and through the acquiring company, only certain sales and marketing personnel may be permitted to discuss those matters and the exchange of highly technical information may be prohibited.

The risk of disclosure through documents related to either business strategies and plans or sales and marketing can be mitigated by and subjecting those documents to review and approval before disclosure to the acquiring company. Business strategies and plans should be submitted to the trustees, while sales and marketing materials should be submitted to the security officer for approval.

The risk of disclosure through email and telephonic communications may also need to be mitigated. Email can be

monitored by automatically diverting and storing a copy of all emails to and from the acquiring company's domain in a separate folder for review by the security officer. Target company personnel allowed to have discussions with acquiring company personnel can be required to log their phone calls and briefly describe the nature of the conversation. There should be enough detail in the description to identify potential red flags regarding any conversation.

As mitigation of the risk of disclosure of sensitive technology to foreign visitors, access to facilities may be restricted. Such restrictions include an effective visitor access program that identifies and logs all visitors (including citizenship status, person visiting, and reason for visit), requires they be badged and chaperoned while on site, and prohibits physical access to the target company's IP. Visiting representatives of the acquiring company may require special handling and even more thorough documentation.

None of this can happen without training of the target company's personnel to understand their new responsibilities. Such training must be focused, thorough, documented, and repeated on a periodic basis. It should also be tested to ensure it is effective.

These are just a few of the more common mitigation steps CFIUS has required. Additional mitigation measures addressing specific risks of a transaction may be required as well.

If this sounds like a major effort, it is. It will require the dedication of resources to take the steps needed to mitigate the risk and to sustain a compliance program that will reassure the government that the national security interests of the United States are protected.

Better to understand the burdens going in than to be surprised later. Considering the cost and burden of mitigation early in the process will result in more informed decision making and a better understanding of the overall value (and cost) of the deal. It may also prevent the imposition of the most serious mitigation measure of all – a third-party monitor.

J. KEITH AUSBROOK

Senior Managing Director

Keith Ausbrook is a key member of Guidepost Solution's high-profile monitoring and compliance practice. He has led teams reviewing compliance programs in financial institutions around the world. Mr. Ausbrook was also a member of the monitor team reviewing the safety programs at General Motors under a deferred prosecution agreement with the U.S. Department of Justice. Mr. Ausbrook is a distinguished lawyer with an accomplished record of managing complex crises. He has held numerous senior executive

and legislative branch positions where he oversaw homeland and national security policy development and implementation, including serving as the chief lawyer on the House Committee investigating Hurricane Katrina and as Executive Secretary of the Homeland Security Council at the White House.