Compliance Monitor May Help With CFIUS Approval

By **Keith Ausbrook** (September 3, 2019, As published in *Law360*)

Although last year's Committee on Foreign Investment in the United States final reform bill walked back some of the original proposed coverage expansions, that isn't going to make it easier to secure approval of acquisitions of U.S. technology by Chinese entities. And expanding coverage to cases where a foreign acquirer does not take control of a target — but can exercise influence — adds scrutiny to transactions that were not previously covered.

Approval of an acquisition may not hinge as much on the extent to which the technology is critical to national security — because that is a given — as it will on whether and how to convince the government the technology can be protected if the deal is approved.

Even before these new provisions were enacted, the CFIUS process was called opaque and secretive. The lack of standards for "exercising influence" could make it more so. Anyone entering the CFIUS black box should do so fully prepared to meet multiple challenges.

Offer a Mitigation Plan Early in the Process

Companies would be well advised to introduce the idea of a mitigation plan at the beginning of the process, not merely hope to avoid it and agree to it as a last-minute concession. When such a plan is offered at the end of the process, it may already be too late — the government's concerns may be unresolvable by then.

A well thought out mitigation plan to prevent the transfer of technology or disclosure of related critical information may be essential to convincing the government that the technology will be protected.

A mitigation plan and its implementation must not come across as mere window dressing to satisfy regulators. Acquirers should be able to demonstrate full understanding and acceptance of their serious responsibility to protect the national security interests of the United States.

They should also demonstrate a sound understanding of the accommodations required both to reassure regulators that the technology will not be transferred and to ensure that they understand, and are willing to bear, the real burden on business operations.

The impact includes new physical security procedures, information security practices that limit communications even within the company, and board and executive obligations for managing the process and reporting to the government.

Enter the Monitor

To demonstrate their full understanding and acceptance of their responsibilities, acquiring companies could commit to engaging a monitor. This shows a willingness to provide an independent perspective on the company's efforts and level of success in protecting the technology and reporting to the government on implementation of the mitigation plan.

Transparency will be essential to ensure the monitor has visibility into the targeted areas of the implementation of the plan. The monitor can reassure the government that the company is in compliance with the mitigation plan only if the monitor has full access to the company's processes for implementing such plan.

Accordingly, the company will need to quickly educate the monitor on U.S. operations and how it plans to fully integrate the mitigation plan into operations and effectively prevent improper transfers and disclosures. This initial education will require the company to give the monitor access to company organizational documents, corporate leadership, facility and information security officials, technology control personnel, and corporate compliance policies and procedures.

At the same time, the monitor will consult with the government to understand its expectations. As a result, gaps and possible inconsistencies with current operations or compliance programs could be identified, requiring additions or modifications to the company's implementation plan at the beginning of the monitorship.

Planning for Success

The mitigation plan will only be successful if it has the full commitment of company officers and directors. Management should be prepared to issue communications that express that commitment to every affected business unit and every level of the company, making clear that violations of the plan will have severe consequences.

Even in a company where the protection of security sensitive technology and information is already an important part of company culture, significant changes may be necessary to ensure the technology is segregated from new owners. Building that culture will be a key element in the success of the plan.

Companies must also pay close attention to ensuring the adequacy of personnel assigned to enforcing the terms of the mitigation plan. The number, qualifications, and proper deployment of personnel will say much about the company's commitment to the plan. The board itself will require new procedures for receiving information about the plan's operations and reporting violations to the government.

The technology control plan is the heart of any mitigation plan. The company is also likely to need supplemental facility access controls, employee access controls and visitor access controls for the covered technology. The monitor will review and evaluate the effectiveness of those controls.

Because information is easily shared through electronic media and can be shared without detection, the company will need to adopt an effective electronic communications plan.

Such a plan will include basic security policies and procedures, awareness and training plans for relevant employees, proper configuration and maintenance of electronic communications systems to segregate protected technology and information, incident management processes and plans, and record-keeping and audit capabilities to enable full reporting on compliance.

Finally, a mitigation plan is likely to disrupt the planning of ordinary business meetings or the co-location of facilities that would ordinarily be recognized as gains in efficiency from a merger or acquisition. Because of security concerns, companies must develop visitation plans to limit access to facilities for non-US persons and facility location plans to prevent the easy sharing of protected technology or information through affiliated offices.

Closing the Deal

It is no surprise that many companies try to avoid a mitigation plan. Given the multiplicity of controls, it can be a costly and burdensome exercise. New or duplicated procedures and

systems can inhibit efficient business operations, and the monitor alone can be expensive and introduce friction into the system.

Nevertheless, it is a fact of life that CFIUS approval is not readily forthcoming, especially in Chinese acquisitions of U.S. technology companies. A company needs to take a hard look at the benefits of an acquisition to determine whether it can bear the burden of a mitigation plan.

If it can, then proposing one — with all the attributes listed above — to the government in the early stages may be the ticket to approval. In many cases, the price of the mitigation plan will be a small price to pay to gain approval.

J. Keith Ausbrook is the senior managing director of Guidepost Solutions LLC.