Guidepost

WHAT TO PREPARE FOR AND EXPECT WITH A CFIUS MONITOR?

Given the recent expansion of transactions subject to review by the Committee on Foreign Investment in the United States (CFIUS), more foreign investments and acquisitions of US-based critical technology and data companies will need to be concerned about the government review. Through the CFIUS review process, the government is attempting to mitigate US national security risks by foreign acquisition or investment in US-based companies which develop critical technologies or have access to sensitive US person data. Additionally, specific real estate acquisitions could be subject to CFIUS review if they allow a foreign entity access through closer proximity to sensitive sites, such as military bases or research facilities.

With these changes, CFIUS is becoming more broadly discussed and understood, and many law firms and financial institutions are working to educate and prepare their clients for the often-rigorous compliance demands of a CFIUS "covered transaction." In certain situations, a foreign investment or acquisition of US-based critical technology, data, or property may be approved by CFIUS but with the requirement that a third-party monitor be used to ensure compliance with any national security-based mitigation agreements. The duties of a third-party monitor include reporting any concerns relative to national security to the government agency overseeing the mitigation plan.

Given the potential for additional oversight by CFIUS, what practical ways can companies prepare for and take advantage of mandated third-party monitors under CFIUS?

1. Know your reality. Many companies which fall under CFIUS review can easily be overwhelmed with the government's expectations. As the CFIUS process gets started, take time to educate your company about the requirements and the work to come. Working with the government to develop a plan which is consistent with its goal of protecting national security while still allowing you to do business can be complicated, but is possible.

2. Leadership must be committed. Your company's leadership must be committed to complying with government requirements. This will be demonstrated from the very beginning of the discussions with CFIUS, and the government will look not only at the capability of the company to comply but also its willingness and commitment by its leaders. As with many things in business, the rest of the company will look to leadership for direction and guidance.

3. Know what needs to be protected and protect it. Do a good self-assessment early in the process to understand what needs to be protected and where your gaps are. You will know from the approval process the specific things the government will want protected. It might be a specific piece of technology or code. It might be specific information such as US citizen personal identifying

information. It could even be access by foreigners to a property given the new provisions around real estate. Knowing what the government values and wants to protect will allow you to start thinking through logical protections in advance of a formalized mitigation plan or agreement.

4. Conduct appropriate due diligence. If your company produces, designs, tests, or develops a critical technology as defined by CFIUS, the government will be interested in how you vet and manage those who have access to the technology. Conducting appropriate due diligence for staff, contractors, and vendors will be built into government mitigation plans. In specific instances, the government will have US citizen requirements for those with direct access. While many technology firms are staffed with a global workforce, companies should be prepared to articulate how it will segregate its workforce and identify potential concerns.

5. Choose a good third-party monitor. Complying with US government compliance agreements can be a lot of work. The role of the monitor is to reassure the government that the company is doing what is needed to comply with CFIUS requirements. The monitor can assist the company in the development of policies and procedures and also provide recommendations for specific controls and best practices. You can expect that your monitor will also have direct communication and possibly a mandated reporting requirement to the government agency responsible for overseeing implementation of the mitigation plan. The relationship between company and monitor can either be a good, collaborative one or it can become adversarial. Choose a good partner in your third-party monitor you can work with positively. Every monitor has a different style; get recommendations and interview them making sure their approach matches your needs. You will need a monitor who has a good working relationship with a number of government agencies and one who is available to you for counsel when you have questions, not just there when you have issues.

6. Staff the efforts. Complying with CFIUS requirements will require work. Addressing the mitigation plan is an "all hands" effort. It will likely involve your information technology, physical security, compliance, legal, and human resource entities. Plan for all employees, contractors and vendors to be trained on the requirements. Many companies struggle with managing all the different aspects of the work required; when possible, consider someone who can lead the CFIUS compliance efforts with appropriate authority, availability, expertise and support across the enterprise.

7. Be patient. The first year of implementing a compliance structure consistent with the government requirements can be taxing. It will take work, communication, and new controls which will need to be socialized, trained to, and tested to make sure your company can comply. Use your government monitoring agency's involvement to your advantage and rely on the expertise of your monitor to help you through the process.