Harvard Law School Forum on
Corporate Governance and Financial Regulation

Successful CFIUS Monitorships

Posted by Randall H. Cook, Mona Banerji, and Steve Klemencic, Ankura Consulting Group, on Monday, July 23, 2018

Tags: Boards of Directors, CFIUS, Cybersecurity, International governance, Oversight, Risk management
More from: Mona Banerji, Randall Cook, Steve Klemencic, Ankura Consulting

Editor's Note: Randall H. Cook is Senior Managing Director, Mona Banerji is a Director, and Steve Klemencic is Managing Director at Ankura Consulting Group. This post is based on an Ankura memorandum by Mr. Cook, Ms. Banerji, and Mr. Klemencic.

This post describes critical considerations for a successful monitorship of mitigating controls required by the Committee on Foreign Investments in the United States ("CFIUS" or the "Committee"). CFIUS is an **interagency US Government committee** that reviews Foreign Direct Investment ("FDI") into the United States to identify and address any consequent national security risks. Growing concern with the impact of foreign countries acquiring national security-critical technologies and other strategic advantages through investment activity has **prompted CFIUS to become more active and assertive**. Moreover, **legislation is pending** in both houses of Congress that will significantly expand CFIUS's jurisdiction to review FDI and require mandatory declaration of specified investment types.

When CFIUS identifies possible national security risks arising from a reviewed transaction, the Committee may make implementation of mitigating control measures a condition of allowing the deal to go forward. In order to assure the effectiveness and persistence of such measures, CFIUS often requires the concurrent appointment of an independent third-party monitor ("TPM") to oversee and periodically report on these controls. Indeed, given the **increasing demands on scarce CFIUS resources** consequent to the policy trends described above, both the Committee and industry are increasingly looking to TPMs to play a critical facilitating role to enable valuable transactions to proceed while addressing national security concerns.

So, what makes for a successful monitorship? Since no two CFIUS related transactions are the same, each monitorship is unique to the facts and dynamics of the transaction on which it is based. However, there are certain features that are foundational to a successful CFIUS monitorship. To best achieve the purposes of CFIUS mitigation agreements, the monitorship needs to be designed, and the TPM selected, with four key considerations in mind: CFIUS experience, technical capability, business cognizance, and trust.

CFIUS Experience

CFIUS may require mitigating controls to address risks identified during a **national security threat assessment that focuses on the foreign party and a vulnerability assessment that focuses on the US party in a covered transaction.** These transactions are becoming increasingly complex **in terms of business organization and ownership**, the technologies and assets at issue, and the corresponding risks presented to US national security. Depending on the nature of the business and assets involved, these risks may include (among numerous other concerns):

- Access to or influence over critical technologies or infrastructure;
- Sensitive supply chain integrity;
- Access to quantities of personal identifying information (PII) or personal health information (PHI);
- Communication and financial network security; and

- Insight into or the ability to monitor sensitive US security and intelligence operations.

A successful CFIUS monitorship must assure the Committee's designated monitoring agencies that the required controls are being implemented effectively and persistently to address the identified risks. Thus, it is crucial that the TPM have a deep understanding of the process, equities, and concerns that underlie the controls, and how the controls need to operate and be reported to address these issues. It is also enormously helpful for the TPM to be thoroughly familiar with the monitoring agencies' process for keeping tabs on mitigation controls, and know how to effectively and efficiently inform the agencies that the underlying national security risks continue to be addressed.

Technical Capability

In order to mitigate complex risks, CFIUS frequently requires a combination of management, technical, and operational controls. Areas where the CFIUS frequently requires mitigating controls include:

- *Access:* Measures intended to limit access to sensitive data, critical technology, and operational information, including:
    - Physical Controls: Limitation of access to company facilities through such measures as electronic badging, camera surveillance, physical barriers, and personnel screening.
    - Systems Controls: Limitation of access to sensitive information and critical controls through such measures as (among numerous others):
        - Partition of business technology systems;
        - Demonstrated compliance with best practice standards for cybersecurity and technology security (e.g., NIST, ISO);
        - Enhanced network security monitoring;
        - Persistent suppression and/or deletion of sensitive information in business systems and processes; and
        - Active penetration testing of both physical and network environments.
- *Protocols and Procedures:* Comprehensive updates to *company policies, processes, and systems* to integrate the requirements of the mitigation agreement to integrate the requirements of the mitigation agreement into the company's governance, operations, and culture. Examples of protocols that facilitate a CFIUS monitorship include:
    - Management protocols that clearly define roles and duties,
    - Data and cybersecurity governance procedures,
    - Third -party vendor assessment and management procedures,
    - Data use and handling policies,
    - Electronic communications protocol, and
    - Incident response protocol.
- *Training:* Programmatic, tailored education of company personnel regarding the purposes and requirements of the mitigation agreement, specifically including individual responsibility for compliance and incident reporting.
- *Incident Response and Reporting:* CFIUS mitigation agreements always require processes to identify, promptly respond to, and notify the Committee of the violation or failure of a mandated control.

A TPM that integrates the right technical competencies with practical experience designing, implementing, auditing, and overseeing compliance with mitigation controls is crucial to success. Required capabilities may include: cybersecurity and response, data and privacy management, data analytics, business process improvement, re-engineering, and automation, forensic auditing and investigations, project management, and regulatory expertise. A seasoned TPM provides critical hands-on guidance and assistance to the company as it works through the practical problems of implementing and

integrating mitigation controls. Concurrently, a technically-competent TPM will be able to credibly demonstrate to the CFIUS monitoring agencies the effectiveness of the monitorship program.

Business Cognizance

By definition, the original impetus for a CFIUS-reviewed transaction is an underlying business proposition that drives the opportunity for a deal. The mitigating controls and monitorship will operate in the context of what all parties anticipate will be a successful business organization. The controls and monitorship must be effective at addressing the identified national security risks, and they also need to enable the company and its people to successfully operate. A successful TPM will recognize that those twin objectives are frequently best-achieved by working with business leaders and operations teams to integrate compliance requirements into corporate structure, systems, and processes. By uniting CFIUS compliance with organizational DNA, the company and the monitorship have the best opportunity for success. Operationally, the TPM needs to have a good understanding of the business and its commitments, and an innovative, risk-based approach that enables achievement of the monitorship's purposes without unnecessarily exercising the company or the CFIUS monitoring agencies.

Trust

Successful CFIUS monitorships are built on a foundation of trust among the parties and the monitoring agencies. The TPM plays the crucial role of honest broker for all equities in this trust relationship. The TPM needs to have the Government's confidence that national security concerns will be addressed with the same energy as would be the case if the monitoring agencies were directly executing the monitorship. Similarly, the TPM needs to have the business's trust that the monitorship's purposes will be addressed with an approach that harnesses innovation and pragmatism to avoid unnecessary friction. To earn and sustain this trust, the TPM needs several characteristics:

- Aa well-earned reputation for integrity and independence,
- A commitment to transparency and open communications with the parties and monitoring agencies,
- A collaborative, engaging approach to executing the monitorship, and
- Consistent, disciplined, and known processes for identifying and resolving issues and monitorship reporting.

Conclusion

The policy dynamics and anticipated statutory changes that are driving increased CFIUS activity are unlikely to abate. Deals involving US companies and FDI with a nexus to national security are increasingly likely to become subject to CFIUS review. When a monitorship is required, integrating the considerations described above in the design of the monitorship and the selection of the TPM will substantially improve the prospects for a successful transaction.
