wiley

ALERT

Department of Justice Announces Increased Monitoring and Enforcement of National Security Agreements Under Team Telecom and CFIUS

July 21, 2020

On July 17, 2020, John Demers, the Assistant Attorney General for National Security, announced that the U.S. Department of Justice (DOJ), as well as other Committee on Foreign Investment in the United States (CFIUS) and Team Telecom agencies, have augmented their staff and begun to more closely monitor and enforce National Security Agreements which have been entered pursuant to CFIUS and Team Telecom. CFIUS and Team Telecom are inter-agency bodies which review certain transactions which involve foreign ownership to identify and address potential national security concerns. It is estimated that hundreds of companies have negotiated such National Security Agreements over the past 20 years.

Mr. Demers' announcement of increased monitoring and enforcement comes on the heels of a lengthy report from the Senate Permanent Subcommittee on Investigations (PSI) finding that, due to a dearth of resources and statutory authorities, government officials "exercised minimal oversight" of the risks posed by Chinese telecom companies. Clients are urged to closely track and document their compliance with existing national security risk mitigation agreements to successfully demonstrate compliance during potential CFIUS and Team Telecom inquiries.

Mitigation Agreements

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Brandon J. Moss
Partner
202.719.7554
bmoss@wiley.law

Practice Areas

Committee on Foreign Investment in the United States (CFIUS)
Government Contracts
International Trade
National Security
Team Telecom
Telecom, Media & Technology
White Collar Defense & Government Investigations

In his keynote address at the American Conference Institute's 6th National Conference on CFIUS, Mr. Demers went beyond the typical policy discussions about CFIUS review and provided important insight into how DOJ and other agencies view mitigation agreements, as well as how CFIUS and Team Telecom plan to monitor and enforce compliance. As a starting point, the number of mitigation agreements monitored by CFIUS and Team Telecom has more than doubled since 2012—an upward trend the Assistant Attorney General described as showing "no signs of abating." Accordingly, CFIUS and Team Telecom have "staffed up" and doubled-down on their efforts to craft effective mitigation agreements, monitor compliance with them, and, when necessary, take enforcement actions to protect national security interests.

Mr. Demers stated that bedrock requirement for mitigation agreements is trust. If the government does not "trust" a party to comply with the mitigation agreement, it will likely not approve a transaction. Examples of such situations include when the party is owned by a foreign government that CFIUS or Team Telecom do not trust, is under the jurisdiction of a government that is not subject to the rule of law, or could be compelled by a foreign government to take action in violation of a mitigation agreement. At base, Mr. Demers stated that even the most thoughtfully-crafted mitigation agreement will not sufficiently mitigate risk if the party signing it cannot be trusted to comply.

Beyond the foundation of trust, and consistent with the recent amendments to CFIUS codified in the Foreign Investment Risk Review Modernization Act (FIRRMA), CFIUS evaluates prospective mitigation agreements from the prism of whether they are "effective, verifiable and enforceable." To that end, it examines them with an eye towards determining how the potential obligations and commitments might work in the "real world." It also asks whether the agreement is "reasonably calculated to be effective," with a particular inquiry into whether the agreement takes into account the motives for the transaction and the parties' incentives. Additionally, it strives to make sure that compliance with the perspective agreements can be "meaningfully monitored" and verified.

Echoing language used by DOJ's Criminal Division and Fraud Section with respect to their evaluations of compliance programs, Mr. Demers stressed that there is no one-size fits all "off the shelf" mitigation agreement that will work for every transaction. However, CFIUS and Team Telecom will expect most mitigation plans to have certain common characteristics, including:

- **Internal Compliance Oversight:** Broadly speaking, mitigation agreements must have provisions requiring sufficient internal compliance controls and procedures. Such controls and procedures may be scaled up or down depending on relevant circumstances associated with the company at issue, the ownership interests, and the perceived national security risks associated with the transaction. Companies entering mitigation agreements should not be surprised to see requirements for things like security directors or officers who are both "appropriately resourced" to enforce compliance and that have direct reporting lines to senior management.
- **External Compliance Oversight:** The government expects that mitigation agreements will include provisions that require companies to independently verify compliance obligations. Such independent verification requirements will likely vary based on the complexity of the business and the potential for

latent violations, but may include imposition of third-party monitors when the agreements pertain to particularly specialized industries—like accounting or technology.

- **Engagement with Monitoring Agencies:** Finally, mitigation agreements should provide for meaningful engagement with monitoring agencies. Transparent and prompt communication regarding material obligations under the agreement is an important touchstone for the government—perhaps out of necessity given the number of agreements monitored by the Department has increased by over 135% over the last decade. Engagement should not be limited to communicating when things go wrong, but extend to supporting site visits and providing meaningful access to key documents and people.

While a lot goes into crafting an effective and enduring mitigation agreement, threat vectors and business practices may change in ways that undermine the agreement's ability to sufficiently mitigate risk. This may be particularly true in situations where agreements are a decade – or multiple decades – old. Recognizing this reality, Mr. Demers made it clear that DOJ and the other constituents reserve the right to go back and revise such agreements to ensure that they properly address current risk realities.

Compliance Monitoring

Mr. Demers also used the speech to provide additional insight into the monitoring of mitigation agreements by CFIUS and Team Telecom. As a jumping off point, he identified the recent Team Telecom Executive Order and FIRRMA passage, collectively, as "an important inflection point in the approach of the Department to mitigation."

Just as there is no "one-size-fits-all" approach to mitigation agreements, the government's monitoring of compliance will differ based on the nature of the business, the characteristics of the parties, and any prior compliance history. That said, while they can be wielded differently given the applicable circumstances, CFIUS and Team Telecom rely on the following key tools when monitoring:

- **In-Depth Site Visits:** A type of monitoring Mr. Demers views as "central to our mission," site visits are designed to provide a boots-on-the-ground view of compliance operations—not merely conference room meetings with PowerPoint presentations. While such visits can be resource intensive, Mr. Demers stressed the importance of seeing technologies and security features in action, inspecting physical premises, and engaging in meaningful dialogue with key officers and staff. Thirty-five site visits were conducted last year, and while coronavirus (COVID-19) has temporarily restricted the visits, he expects that the frequency of such visits will continue to increase given recent expansions to the compliance and enforcement team.
- **In-House Security Directors/Officers:** Mitigation efforts also rely heavily on company-based security directors and officers having substantial independence to inform the government when issues arise. Described as "boots on the ground" for the mitigation team, personnel in those roles provide an important access point for CFIUS and Team Telecom to conduct interviews, seek information, and, if necessary, impose additional monitoring or compliance measures.

- **Mandatory Reports and Notifications:** Finally, Mr. Demers made it clear that the mitigation team takes its review of annual or situational reports and notifications very seriously. In his view, such reports give the government "a helpful view into a company's compliance program, and whether the company has been treating compliance as a year-round exercise or a mere deliverable that must be turned in before the year ends . . . just like a college professor, we can tell when something was thrown together at the last minute."

Enforcement Actions

To properly contextualize the role of mitigation agreements and monitoring, Mr. Demers also reminded the audience of what can happen when things go wrong by highlighting three recent enforcement actions associated with mitigation agreement violations.

Remarking on two recent CFIUS enforcement actions, one resulting in a $1 million civil penalty and the other a $750,000 penalty, Mr. Demers noted that both fact patterns involved "the systematic failure to appropriately resource and support [] compliance obligations." Specifically, both companies failed at having a compliance culture suitable to ensure compliance with the obligations they undertook in their mitigation agreements. In one instance, the company breached its agreement by failing to establish appropriate security policies and failing to honor its reporting obligations to CFIUS. In the other, the company violated a CFIUS interim order by not appropriately restricting and monitoring access to protected data. While both resolutions came at a substantial cost, the penalties likely could have been steeper as Mr. Demers later remarked that the penalties associated with recent enforcement actions "reflect significant discounts" due to cooperation between the companies and the enforcement bodies.

Mr. Demers also highlighted the recent headline-making action taken against a U.S. subsidiary of China Telecom. When discussing the factors that went into Team Telecom's extraordinary decision to recommend revocation of that entity's FCC license, Mr. Demers pointed out that the entity not only failed to comply with its 2007 mitigation agreement, it made inaccurate statements about its storage of U.S. records and its cybersecurity policies—facts DOJ learned through its mitigation monitoring program. Further, the company's operations provided opportunities for the Chinese Government to engage in "malicious cyber activity enabling economic espionage and disruption and misrouting of U.S. communications." Mr. Demers stated that the biggest factor in seeking license revocation as opposed to amending the mitigation agreement to include additional terms was the overriding sense that the company could not be trusted to abide by such terms.

Proactive Corporate Compliance

Companies must take proactive measures to ensure compliance at the earliest possible time. For example, Mr. Demers emphasized that the government should not be the only ones asking probing questions even as early as the negotiation of a mitigation agreement. From the outset, companies must also think carefully about their capability and the cost of complying with the terms and conditions of a proposed agreement, and meaningfully reflect on whether they are in a position to live up to those commitments. Failing to examine whether a company has the necessary resources and wherewithal to comply with an agreement could set it

up for failure, and a resulting enforcement action. Mr. Demers assured the audience that the government is not blind to financial and logistical resources that compliance may pose, and stated that DOJ in particular strives to make requirements manageable. However, at the end of the day, the government's number one concern is national security, and it will use its enforcement powers to ensure that companies are complying with their agreed-to mitigation plans.