Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Companies Will Feel The Weight Of Team Telecom Oversight

By **Megan Brown, Nova Daly and Brandon Moss**
(June 4, 2018, 3:31 PM EDT)

Megan Brown

Nova Daly

Brandon Moss

The federal government is looking at the security of internet, technology and telecommunications companies. This shows up in Congress and across agencies, but includes less-prominent oversight through network security agreements, or NSAs, and other obligations that are imposed as a condition of federal approval of license transfers and other regulated activity, where a company has significant foreign investment or control.

While the Committee on Foreign Investment in the United States often gets the headlines, a lesser-known group called "Team Telecom" wields considerable power. Over 120 companies have entered into publicly available NSAs with the Team Telecom agencies, and many more have reached other accommodations.

For years, Team Telecom has gone quietly about its oversight functions of risk assessment, mitigation and oversight. But as multiple parts of the government grapple with supply chain security, including concerns about Chinese company equipment, companies should anticipate enhanced scrutiny and review their obligations to ensure NSA compliance.

What is Team Telecom?

Team Telecom is a collection of representatives from the U.S. Department of Homeland Security, the U.S. Department of Justice and the U.S. Department of Defense assigned to review foreign investments in U.S. communications assets. Team Telecom examines the national security, law enforcement and public safety issues implicated by proposed transactions. Often Team Telecom will advise that Federal Communications Commission licenses be subject to a company's entrance into an NSA.

Team Telecom has no direct regulatory power. The NSAs are matters of contract, and are made conditions of FCC authorizations. The contracts provide for robust rights of audit and oversight, site visits and the ability to demand documents. They also substantively constrain business decisions and the location of assets.

They afford the government the right to seek liquidated damages and injunctive relief for noncompliance, because parties agree that violations cannot be remedied by monetary relief. For egregious or systemic violations, the FCC may revoke a party's FCC licenses. More and more, companies feel the weight of Team Telecom oversight, which can be burdensome and ongoing.

Scrutiny of Investment and Supply Chains Is Becoming Intense

Numerous agencies, members of Congress and the intelligence community are all raising concerns over foreign influence and control of U.S. telecommunications networks, assets and supply chains:

- Last month, the U.S. Department of Commerce's Bureau of Industry and Security denied the export privileges of Chinese telecom giant ZTE Corp. for seven years after finding that ZTE violated the terms of its 2017 settlement agreement stemming from a multiyear conspiracy to violate U.S. export controls and sanctions laws.

- CFIUS has been much more assertive — for example, blocking Singapore-based Broadcom Ltd.'s hostile bid for Qualcomm Inc., due to concern that the deal would allow China to usurp the United States in the 5G standard-setting process. However, some think CFIUS is inadequately empowered and staffed for the task at hand.

- Congress has introduced the bipartisan Foreign Investment Risk Review Modernization Act, which would expand the jurisdiction and operational mandate of CFIUS and allow it to block more deals involving Chinese buyers. FCC Commissioner Michael O'Rielly recently urged Congress to include reforms to the Team Telecom process as well, as part of this broader legislative effort.

- Congress also is considering legislation that would address U.S. supply chains. One proposal would bar U.S. government agencies from using technology from ZTE and its larger rival Huawei.

- The FCC has launched a rulemaking proceeding that proposes to block the use of federal Universal Service Fund money for the purchase of equipment or services from companies deemed to pose a national security risk to U.S. communications networks or the communications supply chain. The FCC also has tasked an advisory committee — its Communications Security, Reliability and Interoperability Council — with examining supply chain issues; a report is due in September.

- The Department of Homeland Security, a member of Team Telecom, is initiating supply chain efforts that call for increased awareness and scrutiny of telecommunications infrastructure.

Overall, we expect to see increasing scrutiny of foreign investment in the U.S. telecom and IT sectors. This includes activity by Team Telecom.

What to Consider?

Team Telecom agencies can request site visits and documentation, and scrutinize annual filings by NSA signatories. Based on our experience working with Team Telecom over the past 15 years, companies should consider key issues as part of their regular diligence and in expectation of increased oversight:

- The existence and adequacy of policies to ensure compliance with NSA obligations generally
- The existence and adequacy of policies and procedures for IT security and cybersecurity
- Third-party relationships and vendors
- Country of origin throughout the supply chain
- Location of equipment in the United States and overseas
- Location and handling of data
- Third-party and remote access, including through virtual private networks

Who Should Care?

Companies already subject to an NSA

Of course, Team Telecom scrutiny will affect entities with NSAs. As such entities are likely aware, NSAs typically provide Team Telecom with the right to visit facilities and request certain documents and records. Such requests, while seemingly routine, can trigger days and weeks of work: collecting key documents, putting together presentations and investigating potential compliance issues.

Additionally, site visits often require the presence of key employees, removing them from the workforce for multiple days. Even worse, site visits and audits can result in burdensome "recommendations" that may affect business operations and opportunities.

It seems likely that the government's increased interest in network security — especially principal equipment — will drive additional Team Telecom inquiries, site visits and audits.

Entities looking to do business with, invest in or acquire companies with NSAs

As part of its interest in supply chain management, Team Telecom has voiced a growing interest in vendor agreements. While likely not universal, many NSAs include provisions requiring vendors that perform functions covered by the agreement to be notified of the NSA and, sometimes, subject to compliance.

As Team Telecom digs deeper into vendor agreements, companies that work closely with communications providers with foreign ownership interests will likely see more and more notifications of NSA obligations and more burdensome contractual requirements.

Telecommunications and technology companies that are looking for investment by foreign entities or individuals

Increased scrutiny may also affect telecommunications companies that are looking to be partially acquired by foreign entities or individuals. Team Telecom's role in CFIUS proceedings has long been lamented as a burdensome and lengthy process. Indeed, FCC Commissioner Michael O'Rielly recently referenced the lack of structure or deadlines associated with Team Telecom's transactional review

process as a “procedural black hole.”

The added attention around supply chains and foreign infrastructure could exacerbate such issues, and potentially derail sensitive transactions entirely. As such, entities looking to be acquired that may have foreign-made equipment in the critical infrastructure should be cognizant of Team Telecom’s role and increased focus.

And What Should Those Entities Do?

While questions of NSA compliance are often particularized, a common best practice is to do an internal assessment of the entity’s practices and representations previously made to Team Telecom. Assessments serve two purposes.

First, the assessment will help prepare and lessen the load if or when Team Telecom requests a site visit or initiates an audit. In conducting the audit, the entity will likely compile almost the same set of documents Team Telecom would request in such situations.

Second, the assessment gives the entity an opportunity to get in front of issues that arise from incongruity between practices and representations. For example, if a company has reported in its annual report for the last five years that it has not received requests from foreign governments for call data records, the audit should uncover whether that is correct, or whether a notice of noncompliance is necessary. Assessments of this nature should always be done at the direction of counsel to maintain privilege to the greatest extent possible.

Elements of the Internal Audit

Given the government’s recent articulated interest in supply chains, an important part of that audit will be the development and assessment of the entity’s principal equipment lists. Looking at the network diagram, are there components of key critical infrastructure that are made in foreign countries like China?

Another key aspect of the audit should be an honest assessment of vendors. Is the entity outsourcing obligations under the NSA to third parties? If so, are the third parties cognizant and compliant with the terms of the NSA?

Finally, the audit should include a careful assessment of the entity’s standing policies and procedures. Are they in line with the NSA? Are there policies in place to implement each NSA requirement? And, most importantly, are procedures designed to implement or effectuate the NSA followed?

Conclusion

The government takes security of critical infrastructure, including communications networks, seriously. When looking for a stick to ensure security, it is not unreasonable to conclude that Team Telecom will be a natural choice — to the extent an entity is subject to an NSA. As such, entities under NSAs should take a fresh look at their compliance practice.

Additionally, companies doing business with companies subject to NSAs should expect more frequent requests for information and more burdensome contractual provisions when working with those NSA-covered companies.

Finally, entities looking to acquire U.S. communications assets should double down on due diligence, lest Team Telecom qualms about foreign-manufactured equipment in the target's critical infrastructure torpedo a long-negotiated deal.

Megan L. Brown is a partner, Nova J. Daly is a senior public policy adviser and Brandon J. Moss is an associate at Wiley Rein LLP. *The authors wish to thank Wiley Rein attorneys Eve Klindera Reed, Wayne D. Johnsen, Edgar Class, Matthew J. Gardner and Daniel P. Brooks for their contributions to this article.*