PATTON BOGGS LLP

October 9, 2012

Intelligence Committee Calls for Expansion of CFIUS Jurisdiction

Homeland Security, Defense and Technology Transfer Client Alert

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Paul Besozzi
pbesozzi@pattonboggs.com

Stephen McHale
smchale@pattonboggs.com

Jeff Turner
jturner@pattonboggs.com

Dan Waltz
dwaltz@pattonboggs.com

WWW.PATTONBOGGS.COM

On October 8, 2012, the House Intelligence Committee issued a damning bi-partisan report on what it perceived to be national security risks posed by two Chinese telecommunications companies: Huawei and ZTE. The committee strongly recommended that U.S. government and government contractor systems, "particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts."

It further stated that "the Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests." Moreover, "U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects." Of greatest significance, it called for legislation to authorize CFIUS to review purchasing agreements.

CFIUS is an interagency committee charged with determining if a foreign acquisition of a U.S. business could adversely affect U.S. national security. It can require the parties to mitigate any such effects or block the transaction. The parties can also be ordered to unwind the transaction even if it has already been completed. In practice, CFIUS reviews only a small fraction of foreign acquisitions each year because very few have even the remotest possibility of affecting national security.

In cases with obvious national security implications, the parties will often voluntarily bring the transaction to CFIUS following informal discussions. CFIUS can also require the parties to come in and it can and does do so long after a transaction as been completed. CFIUS does not look a foreign "green field" investments or ordinary business transactions, but this could change if the Intelligence Committee's recommendations become law.

The committee's findings are contained in a 60-page public report with an extensive classified annex. It emphasizes what it considers the growing sophistication of cyber attacks emanating from China. It asserts that "Chinese intelligence services, as well as private companies and other entities, often recruit those with direct access to corporate networks to steal trade secrets and other sensitive proprietary data."

After criticizing Huawei and ZTE for being less than forthcoming about their relationships with the Chinese government, the committee finds that there is no way to ensure that the companies' telecommunications equipment has not been compromised. In the committee's view, the risks are increased significantly when the companies enter into managed service contracts giving them access to their customers' sensitive data.

While the report focuses on Huawei and ZTE, its "scope reflects the underlying need for the U.S. to manage the global supply chain system using a risk-based approach." The Intelligence Committee calls for Congressional consideration of "an expanded role for the CFIUS process to include purchasing agreements." It does not limit this recommendation to telecommunications equipment purchases.

If enacted, this would give CFIUS vastly greater powers to intervene in international transactions, far beyond the business acquisition deals it reviews today. Even if this review is limited to purchase agreements by telecommunication network providers and systems developers (Huawei's and ZTE's principal customers), the number of transactions subject to CFIUS review would grow for the low hundreds today to several thousands per year. The need for pre-purchase review would slow commerce and the risk that CFIUS might void a completed purchase could cause to enormous uncertainty.

It is too soon to tell whether this proposal will become law, but it seems clear that transactions involving Huawei, ZTE and other Chinese suppliers of critical infrastructure equipment will be subject to even greater scrutiny. How far this scrutiny will extend beyond China and telecommunications equipment remains unknown, but these developments will need to be closely watched.