On May 15, 2019, Executive Order 13873 was signed to address threats to companies' network security, which potentially could impact companies' trade secrets and everything that keep them profitable and in business. The executive order gives the power to the U.S. Government to block U.S. companies from buying foreign-made telecom equipment deemed a national security. The executive order did not identify the companies of concern, which gives the U.S. Government some latitude (since companies could change names) for enforcement purposes. Threats to network security have been a long-standing issue.

In 2012, the Select Committee on Intelligence for the U.S. House of Representative had issued an unclassified report regarding U.S. National Security Issues Posed by Chinese Telecommunications Companies, Huawei and ZTE. The report recommended:

1) Acquisitions, takeovers, or mergers involving Huawei and ZTE should be blocked, given the threat to U.S. national security interests

2) U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors – particularly those working on contracts for sensitive U.S. programs – should exclude ZTE or Huawei equipment in their systems.

3) Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. And

4) U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.

Please be mindful of the network security issues posed by telecom companies such as Huawei and ZTE; and reach out to us if you are approached by these companies