Chinese Electronics Carry

Steep Risks For Contractors

Related

Sections

- Government Contracts
- Intellectual Property
- International Trade
- Technology

Law Firms

- Crowell & Moring
- Dickstein Shapiro

Companies

- 3Com Corporation
- Huawei Technologies

Government Agencies

- U.S. Department of Defense

Articles

- DOD Contractors Under Fire In Counterfeit Parts Report

Share us on: TwitterFacebookLinkedIn By **Dietrich Knauth**

Law360, New York (October 18, 2012, 7:46 PM ET) -- An ongoing congressional crackdown on Chinese electronic parts in U.S. defense and infrastructure systems has left government contractors stuck between a rock and a hard place: pressured to deliver cheap, commercially available technology on the one hand, and threatened with liability for cyberrisks on the other. The most recent congressional salvo was fired last week in a report from the House Permanent Select Committee on Intelligence that highlighted the risks of espionage and sabotage

posed by unvetted Chinese parts that enter contractors' supply chains. To root out vulnerabilities, contractors must either switch to pricey, military-grade components or conduct expensive testing to ensure commercially purchased products are secure. There's no easy solution to the problem, especially at a time when federal agencies are looking to slash contract spending, experts said. “The supply chain and counterfeit parts is the Achilles' heel of cybersecurity,“ David Bodenheimer of Crowell & Moring said. The Oct. 8 House report focused on Huawei Technologies Co. Ltd. and ZTE Corp., two telecommunications companies with ties to the Chinese government. It urged contractors to avoid doing business with them for fear they could steal U.S. data and turn it over to the Chinese government. The report recommended additional U.S. efforts to block acquisitions, takeovers or mergers involving the companies. It also sought a legislative fix to the risk posed by telecommunications companies that have nation-state ties or that can't clearly be trusted to build vital infrastructure. “Any bug, beacon or back door put into our critical systems could allow for a catastrophic and devastating domino effect of failures throughout our networks,” Committee Chairman Mike Rogers, R-Mich., said. “China is known to be the major perpetrator of cyberespionage, and Huawei and ZTE failed to alleviate serious concerns throughout this important investigation. American businesses should use other vendors.” Even without additional legislation or regulations, the U.S. Department of Defense already has the ability to blacklist certain components and suppliers from its supply chain, Bodenheimer said. That “blunt force” remedy brings its own risks for contractors, especially if the DOD blacklists a particular part or company after a contractor begins to use it during the performance of a contract. “Allowing DOD to exclude certain sources can be draconian,” Bodenheimer said. “For example, if a company should fail to detect the counterfeit parts in the course of screening and end up with those in its system, it could be unable to deliver critical military hardware because those parts have been excluded or blacklisted by the [DOD].” Eliminating Chinese components from contractor

systems can be done, but change will not come cheaply, and contractors' additional costs will surely be passed on to the government, according to Bodenheimer and Steven Lee of Steven Lee & Associates, a firm that specializes in corporate intelligence and investigations related to high-stakes litigation. “The question is really whether or not Congress is prepared to appropriate additional taxpayer funds to obtain alternative — and almost certainly more expensive — components from other 'exotic' sources like U.S. manufacturers with higher quality standards, more transparent manufacturing processes and less incentives to damage the defense infrastructure of the DOD,” Lee said. Though the House report focused on Huawei and ZTE, scrutiny shouldn't be limited to the two companies, but should be turned on others with close ties to the Chinese government, some experts believe. “The vulnerabilities exist, and the risks are real,” Lee said. “It isn't realistic to exclude Huawei and ZTE on the one hand, but fail to exclude a number of other electronics and tactical components makers in China that are even more subject to sovereign influence and that arguably have a higher propensity to provide either shoddy materials or devices loaded with cybercontaminants that lend themselves to sabotage and espionage.” Contractors are already under pressure to avoid Chinese parts after a May Senate report pointed out that bogus Chinese parts had found their way into critical weapons and aircraft, including the Air Force's largest cargo plane. The DOD is preparing new regulations intended to crack down on contractors' use of counterfeit electronics — including a rule that would make them fully liable for the cost of replacing any counterfeit parts. In the days after the House intelligence committee's report was released, Huawei, ZTE and the Chinese government pointed out that it contained no "smoking gun" confirming that Huawei and ZTE had engaged in espionage or intellectual property theft. But based on other evidence of cyberattacks and intellectual property violations from China, lawmakers have every reason to be skeptical of the Chinese government's denials, according to Bodenheimer and Lee. “The

conclusion, to me, is wholly unsurprising," Bodenheimer said. "China has a published doctrine of establishing cyberdominance by 2050. Corrupting the supply chain and building back doors into electronic components is part of that doctrine." In a worst-case scenario, Chinese companies could build components that allow remote unauthorized access and back doors that could corrupt a military system, steal critical information, or even "allow the Chinese to take over our drones and turn them against us," Bodenheimer said. He pointed to the case of a U.S. drone downed over Iran that may have been knocked out by an Iranian cyberattack. China not only has more experience in cyberwarfare, but also has much more opportunity to fill the U.S. supply chain with parts that would allow it to corrupt military systems or critical infrastructure, he said. "Given that the Chinese are far more sophisticated on cyberespionage and cyberattacks, we have to assume that they have the capability to turn our electronics against us," Bodenheimer said. While Congress continues to raise new alarms about Chinese cyberthreats, some say the lawmakers' scrutiny has more do with political tensions than any concrete evidence of danger. David Nadler, a partner in Dickstein Shapiro LLP's government contracts practice, was skeptical of the House report, which he says is light on evidence of wrongdoing by the companies, calling it another example of "political hostility against Huawei and ZTE." Nadler pointed out that in 2008, the U.S. Committee on Foreign Investment in the U.S. recommended that the Bush administration block Huawei's proposed acquisition of 3Com Corp., and that subsequent expansion efforts by Huawei in the U.S. have also been opposed for similar reasons. "U.S. government opposition to Chinese telecoms appears to be based more on economic protectionism and currently is also a campaign issue, rather than any verifiable or concrete cybersecurity or espionage concern inherent in Chinese products," Nadler said. "The House report, which was issued after almost a yearlong investigation, contains no smoking guns or specific security threats but rather recommends that contractors avoid Chinese products primarily based on innuendo from the fact that Huawei and ZTE declined to respond

to certain inquiries regarding their strategic plans." But even if the report is more politics than substance, many U.S. companies have already begun avoiding Chinese products for perceived security issues and concerns over intellectual property theft, Nadler said. And the proposed DOD rule on supply chain integrity will further incentivize contractors to avoid them for telecommunications and related product needs, Nadler said. U.S. technology companies will likely take advantage of the report to market themselves as more secure technology options for contractors, he predicted. "U.S. contractors have and can do without Chinese products, and many were already tightening supply chain even before the proposed DOD rule or the House report," Nadler said. "The report — though probably more accurately characterized as a further example of U.S. economic protectionism — will probably continue this trend and will also be used by U.S. companies to promote their sales." -- Editing by Kat Laskowski and Elizabeth Bowen.