U.S. takes swipe at China for hacking allegations

Anne Flaherty, Associated Press

WASHINGTON (AP) -- The U.S. has taken its first real swipe at China following accusations that the Beijing government is behind a widespread and systemic hacking campaign targeting U.S. businesses.

Buried in a spending bill signed by President Barack Obama on Tuesday is a provision that effectively bars much of the U.S. government from buying information technology made by companies linked to the Chinese government.

It's unclear what impact the legislation will have, or whether it will turn out to be a symbolic gesture. The provision only affects certain non-defense government agency budgets between now and Sept. 30, when the fiscal year ends. It also allows for exceptions if an agency head determines that buying the technology is "in the national interest of the United States."

Still, the rule could upset U.S. allies whose businesses rely on Chinese manufacturers for parts and pave the way for broader, more permanent changes in how the U.S. government buys technology.

"This is a change of direction," said Stewart Baker, a former senior official at the Homeland Security Department now with the legal firm Steptoe and Johnson in Washington. "My guess is we're going to keep going in this direction for a while."

Rep. Dutch Ruppersberger, the top Democrat on the House Intelligence Committee, said he supports the restriction and doesn't think it would be too cumbersome for federal agencies. The Defense and Energy departments already are mindful of how its networks are built.

"Anything we can do to call awareness to the fact that we're continuing to be cyberattacked, we're continuing to lose jobs, and that billions of dollars in American money is being stolen," Ruppersberger said in an interview Wednesday.

In March, the U.S. computer security firm Mandiant released details on what it said was an aggressive hacking campaign on American businesses by a Chinese military unit. Since then, Treasury Secretary Jacob Lew has used high-level meetings with Beijing officials to press the matter. Beijing has denied the allegations.

Congressional leaders have promised to push comprehensive legislation that would make it easier for industry to share threat data with the government. But those efforts have been bogged down amid concerns that too much of U.S. citizens' private information could end up in the hands of the federal government.

As Congress and privacy advocates debate a way ahead, lawmakers tucked "section 516" into the latest budget resolution, which enables the government to pay for day-

to day operations for the rest of the fiscal year. The provision specifically prohibits the Commerce and Justice departments, NASA and the National Science Foundation from buying an information technology system that is "produced, manufactured or assembled" by any entity that is "owned, operated or subsidized" by the People's Republic of China.

The agencies can only acquire the technology if, in consulting with the FBI, they determine that there is no risk of "cyberespionage or sabotage associated with the acquisition of the system," according to the legislation.

The move might sound like a no-brainer. If U.S. industry and intelligence officials are right, and China is stealing America's corporate secrets at a breathtaking pace, why reward Beijing with lucrative U.S. contracts? Furthermore, why install technical equipment that could potentially give China a secret backdoor into federal systems?

In late 2012, Ruppersberger and House Intelligence Committee Chairman Mike Rogers, a Republican, released a report urging U.S. companies and government agencies to drop any business with Chinese telecommunications companies Huawei Technologies Ltd. and ZTE Corp. because of the security risks they pose.

"Any bug, beacon or backdoor put into our critical systems could allow for a catastrophic and devastating domino effect of failures throughout our networks," Rogers said in a statement accompanying the report.

But a blanket prohibition on technology linked to the Chinese government may be easier said than done. Information systems are often a complicated assembly of parts manufactured by different companies around the globe. And investigating where each part came from, and if that part is made by a company that could have ties to the Chinese government could be difficult.

Huawei, the third-largest maker of smartphones, says it is owned by its employees and rejects claims that it is controlled by the communist government or China's military.

Depending on how the Obama administration interprets the law, Baker said it also could cause problems for the U.S. with the World Trade Organization, whose members include U.S. allies like Germany and Britain that might rely on Chinese technology to build computers or handsets.

But in the end, Baker says it could make the U.S. government safer and wiser.

"We do have to worry about buying equipment from companies that may not have our best interests at heart," he said.

Source URL (retrieved on *12/18/2013 - 10:48pm*):

http://www.ecnmag.com/news/2013/03/us-takes-swipe-china-hacking-allegations