Bond Case Briefs

Municipal Finance Law Since 1971

Local Governments Using a Software That Russia May Be Using for Espionage.

Local and state government agencies from Oregon to Connecticut say they are using a Russian brand of security software despite the federal government's instructions to its own agencies not to buy the software over concerns about cyberespionage, records and interviews show.

The federal agency in charge of purchasing, the General Services Administration, this month removed Moscow-based Kaspersky Lab from its list of approved vendors. In doing so, the agency's statement suggested a vulnerability exists in Kaspersky that could give the Russian government backdoor access to the systems it protects, though they offered no explanation or evidence of it. Kaspersky has strongly denied coordinating with the Russian government and has offered to cooperate with federal investigators.

The GSA's move on July 11 has left state and local governments to speculate about the risks of sticking with the company or abandoning taxpayer-funded contracts, sometimes at great cost. The lack of information from the GSA underscores a disconnect between local officials and the federal government about cybersecurity.

Interviews suggest that concerns in recent months from Congress and in the intelligence community about Kaspersky are not widely known among state and local officials, who are most likely to consider purchasing the Russian software. Those systems, while not necessarily protecting critical infrastructure, can be targeted by hackers because they provide access to troves of sensitive information.

U.S. intelligence chiefs in May told a Senate panel that they wouldn't use the company's software during a broader hearing investigating Russia's alleged meddling in the U.S. presidential election. It was not the first time Congress had heard that message: A former U.S. official told The Washington Post that congressional staff was advised by law enforcement in late 2015 to stop meeting with Kaspersky representatives over national security concerns.

"People need to know that they can trust software updates," said Joseph Lorenzo Hall, chief technologist at the Center for Democracy and Technology, a digital advocacy group. About the GSA's decision, he said: "We need more public information."

In the weeks since Kaspersky's delisting, The Post found that it continues to be used on government computers in jurisdictions ranging from Portland, Ore., to Fayetteville, Ga., where an official said they have a year-to-year contract.

View Full Story From The Washington Post.

GOVERNING.COM

July 24, 2017