Md. must cut ties with Russian-owned ByteGrid

Senate President Thomas V. Mike Miller, House Speaker Michael E. Busch and Nikki Charlson, deputy state administrator for the Maryland State Board of Elections discuss Russian investment in state election system. (Thalia Juarez | Baltimore Sun Media Group)

There's only one way for Maryland officials to do right by voters now: Tear up the state's agreement with its elections contractor and remove their data from the vendor, ByteGrid. Cut it off — immediately.

ByteGrid, a web hosting and data center company based in Silver Spring, reportedly neglected to tell Maryland back in 2015 when Russian investors — including an oligarch with ties to President Putin — bought an ownership stake in the business. Is it possible the company recognized that the high-level Russian connections would cause alarm? Or, even worse: Did they not think it was that big of a deal? That was completely irresponsible behavior, and ByteGrid's after-the-fact security assurances ring hollow.

ByteGrid claims that investors have no access to names of companies or what they do for them. But is it really just a coincidence that a Russian oligarch is investing in data centers that store election information? And if the Russian investors didn't know before, they certainly know now.

Maryland so far appears to be more interested in managing the ByteGrid public relations crisis, however, than in taking the underlying problem seriously. In her July 13 statement about ByteGrid's Russian connection, State Board of Elections Deputy Administrator Nikki Charlson said the board would work with "federal and state partners to develop a plan of action to audit existing data, review existing defenses, and immediately implement any changes to secure the systems and data before the 2018 General Election."

Sorry, Ms. Charlson — it's too late. Once an intruder gains access to a system, it's game over. When you're in, you're in. That's the reality of IT security. Maryland's predicament isn't just a perception problem. Whether or not any Marylanders' data have been compromised so far, why continue to expose voters to the risk? And why trust a company that's already lied to you once, when it now says there's nothing to worry about?

The ByteGrid fiasco is a two-headed snake. One head has its fangs in the election system of a U.S. state, and the other in millions of U.S. residents' personal data. That's a win-win for ByteGrid's owners.

Think of all this from the perspective of a foreign government that wants to influence another nation's elections. Why leave things to chance? Why stop at trying to change voters' hearts and minds via social media or fake news? Just buy a company that owns the actual voting infrastructure — after the company has secured a contract with a state government.

This is a big deal. It's not simply something for the IT industry or election system wonks to discuss on conference panels later this year. We need a modern Paul Revere sounding the alarm: One if by land, two if by sea, three if by cyberspace. It's an urgent wake-up call, not only to state governments but also to Wall Street, Main Street and all our major industries. How many other ByteGrids are out there, undiscovered, potentially affecting federal and state elections?

A year ago, hackers at the DefCon computer security conference in Las Vegas held their first-ever Voter Hacking Village. It took them all of about 90 minutes to reveal how easily voting systems can be compromised.

As for Maryland, why set the bar low? In a time when Russian influence on the American government at the highest level continues to be top-of-mind in the media, not to mention among federal investigators, and when the president himself fueled doubt about the integrity of state voting systems, why allow the Free State's reputation to sink into the muck of suspicion?

The state should have used a company that was 100 percent U.S. owned and staffed. There are plenty of choices (I know, because we're one of them). The potential for mischief is just too high to expose federal or state election systems to foreign actors.

America used to be smarter than this. The Foreign Corrupt Practices Act was passed 40 years ago to stamp out corrupt conduct, particularly regarding foreign influences. The Securities and Exchange Commission vigorously enforces it. Do we need new laws, stronger enforcement, better detection? Maybe. What we really need is integrity and indignation.

Just because our opponents are bold and slick about undermining our sovereign elections doesn't mean we should surrender. No, we need to be equally smart and open-eyed about the risks we face and act without hesitation to defend our systems. Our democracy literally depends on it.

Sonia Sexton (ssexton@mineralgap.com) is chief security officer for New York-based DP Facilities, which owns and operates the Mineral Gap data center in Wise, Va. She has more than 20 years of experience in significant security roles within major federal contracting firms.