

RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:

COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 8, 2019

Mindy Perkins
President, Chief Executive Officer
VR Systems
3773 Commonwealth Blvd.
Tallahassee, FL 32303

Dear Ms. Perkins:

I write to seek information about the hack of VR Systems' computer network in August of 2016 by the Russian government and any possible connection to the catastrophic failure of your products on November 6, 2016, at six polling places in North Carolina, which resulted in voters being turned away.

The Department of Justice recently released a redacted copy of the Report On The Investigation Into Russian Interference In The 2016 Presidential Election by Special Counsel Robert Mueller ("the Mueller Report"), which described how Russian intelligence personnel targeted U.S. election infrastructure. The Mueller Report revealed that in addition to targeting state and local governments, "[t]he GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations."

As part of this Russian government hacking campaign, the Mueller Report states that "[i]n August 2016, GRU officers targeted employees of [redacted], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network." Your company recently identified itself as the unnamed cyber-victim, in a written statement to the Raleigh News & Observer.

The compromise by Russian hackers of your computer systems in August of 2016 is particularly concerning because electronic poll book systems manufactured by your company catastrophically failed in six precincts in Durham County, North Carolina during the November 8, 2016 general election. According to a public statement by the Durham County Board of Elections, the systems that malfunctioned were used to verify voter registrations and to print authorization to vote forms, which voters must sign before they are given a paper ballot. Election officials at several precincts did not have a sufficient number of paper authorization forms on hand, which the polling places switched to after your products failed. This caused one polling location to shut down completely for an hour and a half at lunchtime, a peak period for working voters.

In 2017, election officials in North Carolina attempted to prevent your products from being used to administer future elections because of security concerns. You then sued the state of North

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTP://WYDEN.SENATE.GOV](http://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

Carolina, successfully, to prevent state election officials from revoking your operating license. In court filings as part of that court case, you were asked whether your company had “ever experienced a breach of security regarding EViD [your electronic poll book product].” You responded: “No.”

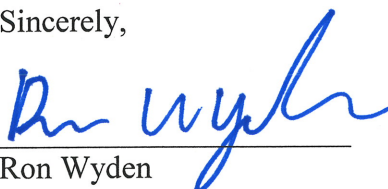
The Mueller Report’s revelation that Russia infected your network with malware raises serious questions about your March 2018 claim your company had not experienced a security breach.

Given the voting problems caused by the failure of electronic poll books manufactured by your company in November 2016, the American people have a right to know if there was any connection to the Russian cyber attack against your company three months earlier. To that end, please answer the following questions by May 16:

1. The North Carolina Board of Elections has stated publicly that it “lacks the necessary technical expertise to forensically analyze the computers used in Durham County, and other government agencies declined the agency’s requests to evaluate them.” Were the VR Systems electronic poll books that failed in Durham County on November 6, 2018 forensically examined for evidence of hackers by cybersecurity experts working for any government agency? If yes, please provide a copy of all reports or assessments shared with your company after the forensic examination of these devices.
2. Your company asserted in a March 2018 court filing that you had not experienced a breach of security. What was the evidentiary basis for this unqualified assertion?
3. Have your corporate computer networks and systems been subjected to a forensic examination to determine the scale and impact of the hack by the Russian government described in the Mueller Report? If no, please explain why. If yes, please provide me with all post-breach analysis, including reports created by private cybersecurity companies and government agencies.
4. On August 1, 2016, did you employ a Chief Information Security Officer, or any other individual with sufficient cybersecurity experience and skills, who was responsible for protecting your systems from hackers? If no, do you employ someone in such a role today?
5. On August 1, 2016, had you implemented the National Institute of Standards and Technology (NIST) cybersecurity framework? If no, have you now implemented the NIST framework?

If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator