



August 30, 2016

Executive Director Strach sends letter to DHS official asking to join DHS cybersecurity monitoring program. Through the program, DHS monitors North Carolina's systems to check for vulnerabilities.

November 8, 2016

Election Day.

January 6, 2017

DHS designates election systems as "critical infrastructure," meaning election infrastructure will be a top priority in cybersecurity assistance from the federal government.

June 5, 2017

The Intercept reports on a classified intelligence report from the National Security Agency suggesting that VR Systems may have been a victim of Russian hacking through a spear-phishing campaign.

June 6, 2017

State Board launches an investigation into alleged attempts to compromise VR Systems' electronic poll book software, which is used on Election Day in 21 counties.

Early to Mid-June, 2017

The State Board and all 21 counties that use VR Systems' software check all email accounts for evidence of spear-phishing from suspect accounts, but do not find any evidence of such attempts.

June 21, 2017

DHS officials testify before Congress that election systems in 21 states were potentially targeted by Russian government cyber-actors. A small number of networks were successfully compromised, while attempts in other states were unsuccessful, they say.

July 20, 2017

State Board sends letter to DHS official asking for any information about any attempt to compromise election systems in North Carolina in 2016.

September 5, 2017

In response to published reports, State Board sends Freedom of Information Act request to DHS seeking all emails and other correspondence from any DHS employees regarding alleged hacking in North Carolina.

September 22, 2017

Department of Homeland Security notifies State Board officials that North Carolina's government-owned election systems were not targeted by Russian cyber-actors.