



State of Vermont

Office of the Secretary of State

128 State Street

Montpelier, VT 05633-1101

[phone] 802-828-2363

[fax] 802-828-2496

www.sec.state.vt.us

James C. Condos, Secretary of State

Christopher D. Winters, Deputy Secretary

October 30, 2018 - For immediate release

Contact: Eric Covey, 802-828-2148

Vermont Secretary of State Jim Condos Assures Vermonters: Your Votes Are Secure!

Montpelier, VT – Today Vermont Secretary of State Jim Condos released the following statement regarding the security and integrity of Vermont elections in advance of the November 6th, 2018 General Election.

“Vermont voters deserve the peace of mind that when they vote early or at the polls on Election Day, they can do so knowing that we have done everything in our power to ensure that their vote is secure and protected.

When 21 state election systems were attacked by Russian cyber agents in 2016 it changed our world as we know it. Now, we’re living under a new normal. For my office, and for Secretaries of State and election officials across the country, cybersecurity is constantly front and center and something we focus on every single day. Vermont is considered one of the leaders in election cybersecurity nationally, in part because we began focusing on cybersecurity starting back in 2013.

We have also been ahead of the curve because our election laws and system of election administration give us the baseline protections necessary to ensure that every vote is counted fairly and accurately, and that we have the redundancies in place to ensure the same even in a worst case scenario.

Ballot Security Basics – the Vermont Advantage

Our most important protection may also be the simplest: every vote cast in Vermont is backed up by a voter-marked paper ballot. Every vote can be audited for accuracy, and in fact we do conduct a post-election audit after every General Election. I consider paper ballots and audits more than a best practice - they ensure our election results can be confirmed as accurate with a high degree of statistical confidence.

Vermont voters may be familiar with the optical scan tabulator machines many Vermont Cities and Towns use to count ballots on Election Day. It’s important to know that these machines are tested rigorously during their certification process with the Election Assistance Commission and by our local municipal clerks before each election.

There is a strict chain of custody for the memory cards used to program the machines. For a hacker to reprogram the memory cards they would need to break into the Town Office, break into the clerk’s office, break into the vault, remove and reprogram the memory card, and get it back in to the vault without raising any suspicion. Even in that case, since the tabulators are not connected to each other or to the internet, either by Wi-Fi, hardwire, or remote access software, I feel confident saying that it would be nearly impossible to hack Vermont’s tabulators in any sort of widespread manner. Our decentralized, town-level elections are yet another simple protection against election tampering. Even if we were to suspect some corruption in the machines, we can always go back to the paper ballots as a failsafe measure. All ballots are sealed and saved for 22 months after the election.

Cybersecurity Protections of Our Election Systems – Behind the Scenes

We’ve completed a considerable amount of work putting the necessary cyber protections in place to defend our Vermont election management systems. Each of our IT solutions have been replaced since 2012 and with each iteration, better and newer technology brings with it stronger cyber-defenses.

Our election management system, voter registration database, and election night reporting website are all protected by web application firewalls in front of all ‘doors’ to our system. We block known or suspected problem IP addresses and whitelist known, trusted users. We have installed an Albert Monitor through our federal partners, which

monitors traffic coming to our websites in real time, and can quickly notify us of any suspicious activity. We receive weekly cyber hygiene scans from the Department of Homeland Security (DHS), and so far these scans have not detected any vulnerabilities.

We have implemented two-factor authentication for anyone who has access to our election management system, including our own staff and the municipal clerks. We've combined this with 'secure the human' trainings. Cyber security experts will tell you that the biggest risk factor is the human factor, which is why we've worked hard to deliver training and education to our local partners. Our municipal clerks are on the front lines of our democracy, and work incredibly hard to ensure access and security for Vermont voters.

Effective cyber security isn't just about keeping the bad actors out, it's also about planning for the worst and mitigating the damage that can be done if a hacker is eventually successful. All computers are vulnerable and no system is 100% secure.

For instance, we back up our voter registration database daily. In a worst case scenario we can always do a 24-hour restore, and even if a voter had registered in that one day window, same day voter registration ensures that they can register at the polls before voting.

No eligible voter will be denied their right to register and cast a ballot.

Federal and State Partnerships – Our Communications Have Dramatically Improved

Since 2016, we've worked hard to increase our communications and information sharing capabilities with our federal partners. While I was skeptical when DHS first announced that elections were to be designated as critical infrastructure, this designation has brought additional resources, like the Albert Monitor and weekly hygiene scans, to states like Vermont.

Through DHS we have access to an Election Day threat dashboard to receive and monitor information regarding potential threats. We have established an Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) comprised of all 50 states and more than 1,300 county or local governments to facilitate information sharing and collaboration on best practices to mitigate and counter threats to election infrastructure.

We are also actively working with the U.S. Attorney, Vermont Department of Public Safety and Vermont State Police. Securing our elections takes a team effort, and I can assure Vermont voters that the partnerships and communication channels we've built between state and federal partners are much improved and are a critical asset in defending our democracy.

Combatting Misinformation and Disinformation

The true aim of our Russian adversaries in the 2016 attacks was to sow chaos and discord, and to weaken voter confidence in the integrity of our elections. Alongside these direct attacks, the spreading of misinformation and disinformation on social media presents as great of a threat.

To that end, both Facebook and Twitter have created direct channels for election officials to report misleading information on and around Election Day so that it can be investigated and removed.

The message I want to impart to voters is that Vermont was in good shape in 2016, and we're in even better shape today. When you go to the polls on Election Day, you can cast your ballot knowing that we have done the work necessary to secure our elections, and ensure that your vote is protected.

If any voter is experiencing issues on Election Day they can call our official Election Day Hotline at 1-800-439-VOTE (1-800-439-8683).

Please join me in voting this year. Your VOTE is Your Voice!"

###

www.sec.state.vt.us | www.facebook.com/SecretaryOfStateJimCondos | www.twitter.com/VermontSOS

