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

June 28, 2017

Hon. Richard Burr
Chairman
U.S. Senate Select Committee on Intelligence
217 Russell Senate Office Building
Washington, DC 20510

Hon. Mark Warner
Vice Chairman
U.S. Senate Select Committee on Intelligence
703 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Vice Chairman Warner,

I have received the letter you sent to National Association of Secretaries of State (NASS) Executive Director Leslie Reynolds. Thank you for your committee's work on this incredibly important matter. As Vermont's chief elections officer, I welcome the opportunity to respond to your letter and highlight my approach to election security along with the many concerns I share with my fellow Secretaries of State.

Voting is the very core of our democracy. Vermonters have every right to elections that are free and fair, with full confidence in their outcomes. As Vermont's chief elections officer, election integrity is my highest priority. This includes the security of our election information and systems.

I was glad to see attention focused on cybersecurity preparedness during last week's Senate Select Intelligence Committee Hearing in Washington. The threat is real and there is ample evidence that Russia has targeted the U.S. elections in an attempt to access multiple voter registration databases.

During the hearing, Dr. Sam Liles, Acting Director of the Cyber Division of the Department of Homeland Security (DHS), told Senators that Russian cyberattacks targeted 21 states during the 2016 presidential election. However, DHS officials then refused to identify which states were involved, or what the targeting activity actually entailed.

While it is true that each day our computer systems defend against many attempts to gain access to our systems, particularly through the use of malware and phishing attempts, this is very different than an actual breach. It is my concern that the spread of misinformation about actual vulnerabilities and breaches only furthers the goal of our foreign adversaries: to undermine the faith we have in our

democracy. False information is being repeated by news media, federal agencies, and is even perpetuated by some of your colleagues in Washington.

I write to you today to ensure that the record is clear regarding the security of Vermont's election systems and processes. Hopefully, this information will be useful to you in your work pursuing fact-based, effective reforms supporting the integrity of our elections:

- The November election was not "hacked." No evidence exists that any vote tallies were changed.
- Foreign intrusions into state and local election boards in 2016 were limited to TWO INCIDENTS (IL & AZ) that did not involve systems used in vote tallying.
- Additional state voter registration systems (21 states, according to DHS) were "targeted" by cyber hackers, but NO ADDITIONAL SYSTEMS were accessed or breached. Vermont was not targeted or breached.
- Vermont and 32 other states took advantage of voluntary cybersecurity assistance provided by the U.S. Department of Homeland Security, while the remaining states utilized in-state/private sector resources available to them. Vermont continues to work with DHS today.
- Our highly-decentralized, low-connectivity elections process in the United States provides BUILT-IN SAFEGUARDS against large-scale cyberattacks.
- Additionally, Vermont has a paper ballot back-up and conducts a post-election audit of the vote. Our post-election audits have provided integrity to our election night vote counts. Not all states require paper ballots as an end product, or a random audit to confirm results.
- I believe you will find all states are working to strengthen their systems for future elections.

The Vermont SOS office anticipated cybersecurity threats and began preparing for them years ago. We were the first state agency to undergo a thorough cyber-security assessment, including penetration testing for all of our data and systems, starting in the fall of 2014.

All elements of our elections system, including our statewide checklist, have undergone extensive reviews and testing for vulnerabilities to cyber threats. Based on the test results, we initiated an aggressive schedule to remedy the findings until all issues were mitigated. We have not detected any attacks of the kind described DHS alerts, though we are constantly monitoring our systems to be on the lookout.

The professionalism of our many municipal clerks and their local election workers make systematic fraud and compromising the system extremely difficult to do. Vermont is one of the many states where a paper ballot is required at the end of the day for review, even if the ballot is run through a tabulator. Our tabulators are maintained and tested for optimal performance before every election. None of our tabulators are connected to the internet or any other software.

It is also important for you to know that we have struggled with a lack of information from DHS ever since these cyber threats emerged last summer. We have heard about breaches second hand through the news media and have only received a trickle of unclassified information about threats and alleged

state victims. It is imperative that chief state election officials across the U.S. receive security clearances as quickly as possible in order to receive timely and specific threat information in order to protect our state systems.

It appears DHS is not yet well-versed on how elections are conducted at the state level and the degree to which Secretary of State's offices are involved and are in charge of elections in most states. You may have heard that our National Association of Secretaries of State (NASS) has issued a statement opposing the designation of elections systems as critical infrastructure due to the unsteady partnership.

We are confident that our elections systems in Vermont are secure, but we remain vigilant for new threats and evolving security needs. To reiterate, the threat is real and no system is invulnerable to tampering. Russian tampering needs to be further investigated and dealt with and hopefully fully acknowledged and taken seriously by the Trump Administration.

I sincerely hope Congress will consider another round of funding like it did with the Help America Vote Act (HAVA) in 2001 to upgrade outdated elections systems with the very latest in functionality and security.

It is also worth repeating that we must be careful with our language and make a clear distinction between being "breached" (only two states) and being "targeted" (21 states, no breaches) when it comes to potentially undermining our democracy. Without free and fair elections, we have nothing.

Thank you – and please feel free to contact me on any issues I may be of assistance.

Sincerely,

Jim Condos
Vermont Secretary of State

Cc: Hon. Senator Patrick Leahy
Hon. Senator Bernie Sanders
Hon. Representative Peter Welch
Hon. Governor Phil Scott
Hon. Attorney General T.J. Donovan