PROPOSED

SENATE AMENDMENTS TO S.C.R. 1037

(Reference to printed resolution)

Page 1, strike lines 1 through 9, insert:

"Whereas, public functions such as voting should be open to the public and transparent except to preserve voter anonymity; and

Whereas, recognizing the vital role of elections in national security, in 2017 the United States Department of Homeland Security designated election infrastructure as critical infrastructure of the United States; and

Whereas, supply chain risks related to manufacturing, assembling and testing critical infrastructure items, including computerized voting machines, can be mitigated by appropriate standards and actions adopted by the United States government; and

Whereas, computerized voting machines and systems used in this state contain electronic components that are manufactured, assembled or tested in foreign nations that pose a threat to the United States and include unsecure components in computerized devices that can and have been used to infiltrate, exfiltrate and manipulate data as discussed in various publications; and

Whereas, actual breaches of computerized devices and computer systems have been discovered at the United States Department of Defense, thousands of government contractors and agencies and Fortune 100 companies, illustrating the threat to computerized systems, including computerized voting machines as noted by the United States Cybersecurity and Infrastructure Security Agency and various media outlets; and

Whereas, the United States Senate Intelligence Committee held a hearing on March 21, 2018 relating to potential foreign interference in the 2016 election; and

Whereas, at the March 21, 2018 meeting Election Systems and Software denied selling voting machines with remote access software, a fact Election Systems and Software later admitted was true in a letter to Senator Ron Wyden; and

Whereas, Election Systems and Software represented to its customers and potential customers that its DS200 voting system was "fully certified and compliant with United States Election Assistance Commission guidelines" even if used with a modem, a critical access point by which unauthorized access can be made; and

Whereas, the United States Election Assistance Commission issued a letter to Election Systems and Software dated March 20, 2020 stating that Election Systems and Software misrepresented that its voting machines with modems complied with the United States Election Assistance Commission requirements and required Election Systems and Software to correct its misrepresentations; and

Whereas, on June 3, 2022, the United States Cybersecurity and Infrastructure Security Agency issued an advisory warning identifying nine critical security vulnerabilities in the Dominion ImageCast X devices and any voting machine components having a direct or indirect connection to that device; and

Whereas, the Dominion ImageCast X devices and any voting machine components having a direct or indirect connection to that device are used in sixteen states, including this state; and

Whereas, the United States Cybersecurity and Infrastructure Security Agency issued a June 3, 2022 advisory warning in direct response to the findings of a recognized computer science expert, Dr. J. Alex Halderman, who had twelve weeks to examine this voting system; and

Whereas, before the United States Cybersecurity and Infrastructure Security Agency's warning, Dr. Halderman filed multiple sworn declarations in federal court attesting that:

1. Certain security failures could be exploited to steal or alter votes while evading all known safety procedures such as logic and accuracy tests and risk-limiting audits; and

2. Dominion ignored Dr. Halderman's requests to meet to seek a remedy for these security failures; and

3. It would take many months for Dominion to try to fix these security failures and obtain United States Election Assistance Commission and state-level approvals for such changes; and

Whereas, Dr. Halderman filed a twenty-five thousand word report with a federal district court detailing the critical security failures related to United States Cybersecurity and Infrastructure Security Agency's June 3, 2022 advisory warning; and

Whereas, Dominion has a copy of that report and has not made or sought the court's permission to make that report available to the public; and

Whereas, the presence of the security failures identified in the United States Cybersecurity and Infrastructure Security Agency's advisory warning would directly prevent computerized voting systems' compliance with voting systems standards; and

Whereas, although the United States Cybersecurity and Infrastructure Security Agency stated in that advisory that it has "no evidence that these vulnerabilities have been exploited in any election," there is no indication that the United States Cybersecurity and Infrastructure Security Agency or officials in this state ever investigated whether computerized voting machines in this state have been exploited through these known vulnerabilities or any other vulnerabilities; and

Whereas, the United States Cybersecurity and Infrastructure Security Agency's June 3, 2022 advisory warning identified thirteen defensive measures that have not been undertaken in this state; and

Whereas, computerized voting machines used in this state are unsecure, lack full public transparency and deprive voters of the right to know that their votes are counted and reported in an accurate, auditable, legal and transparent process; and

Whereas, on November 3, 2021, the Tennessee Secretary of State's office reported to the United States Election Assistance Commission that an "anomaly" was observed during a municipal election in Williamson county, Tennessee, which used Dominion tabulators for a municipal election; and

Whereas, the Tennessee anomaly caused the scanners to mislabel valid ballots as provisional, and therefore did not include these ballots in the poll report totals; and

Whereas, after conducting a formal investigation of the Tennessee anomaly, the United States Election Assistance Commission issued a report on March 31, 2022 concluding that the "anomaly" was likely rooted in "erroneous code" present in Dominion's system; and

Whereas, there was no conclusion in the United States Election Assistance Commission report on how the "erroneous code" came to be on the voting machine, or how such code was not detected in the certification process or other safety testing procedures; and

Whereas, instances of computerized voting machine failures to accurately record vote totals have repeatedly occurred since 2002 and continue to occur to this day; and

Whereas, because of the lack of transparency and detailed public postelection audits of computerized voting machines, there is no way to tell how many times inaccurate election results have been wrongly certified; and

Whereas, the United States government employs open source technology to foster transparency; and

Whereas, the source code used to read and tabulate ballots in computerized voting machines used in elections in this state for federal office is not open source and not openly available to the public to evaluate that code for malicious activity; and

Whereas, Article I, Section 4, Clause 1 of the United States Constitution empowers state legislatures, including the legislature of this state, to prescribe the "Times, Places and Manner" of conducting federal elections; and

Whereas, the definition of "manner" is at the sole discretion of the legislature; and

Whereas, Article II, Section 1, Clause 2 of the United States Constitution empowers state Legislatures, including the legislature of this state, to direct the manner of appointing electors for President and Vice President of the United States."

Page 1, strike everything after the resolving clause and insert:

"That no voting system or component or subcomponent of a voting system or component, including firmware software or hardware, assemblies and subassemblies with integrated circuits or on which any firmware or software operates, may be used or purchased as the primary method for casting, recording and tabulating ballots used in any election held in this state for federal office unless:

1. All components have been designed, manufactured, integrated and assembled in the United States from trusted suppliers, using trusted processes accredited by the Defense Microelectronics Activity as prescribed by the United States Department of Defense; and

2. The source code used in any computerized voting machine for federal elections is made available to the public; and

3. The ballot images and system log files from each tabulator are recorded on a secure write-once, read-many media with clear chain of custody and posted on the Secretary of State's website free of charge to the public within twenty-four hours after the close of the polls; and

4. The legislature transmits this resolution to the secretary of state."

Amend title to conform

SONNY BORRELLI

SCR1037BORRELLI.docx
02/09/2023
01:46 PM
C: CT