

COMMITTEE ON ELECTIONS
SENATE AMENDMENTS TO S.C.R. 1037
(Reference to printed resolution)

1 Page 1, strike lines 1 through 9, insert:

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

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

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

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

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

1 Whereas, the United States Senate Intelligence Committee held a
2 hearing on March 21, 2018 relating to potential foreign interference in the
3 2016 election; and

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

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

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

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

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

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

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

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

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

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

12 Whereas, Dr. Halderman filed a twenty-five thousand word report with
13 a federal district court detailing the critical security failures related
14 to United States Cybersecurity and Infrastructure Security Agency's June 3,
15 2022 advisory warning; and

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 3. The ballot images and system log files from each tabulator are
2 recorded on a secure write-once, read-many media with clear chain of
3 custody and posted on the Secretary of State's website free of charge to
4 the public within twenty-four hours after the close of the polls; and
5 4. The legislature transmits this resolution to the secretary of
6 state."
7 Amend title to conform

SCR1037ELEC.docx
02/09/2023
01:46 PM
C: CT