Top Five Reasons Florida Needs
the “Election Technology Security” Bill

The adoption of enterprise-class technology and data communications in Florida’s elections has outpaced its laws. Enacting Senator Garcia and Representative Barnaby's 2025 session bills (SB394/HB1203) ensures Florida is the gold standard for election technology security again!

1) Enterprise-class technologies used throughout Florida’s election process are not subject to the important controls Florida law puts in place for “voting” system security. This means enterprise- class technologies are not certified by the state, are not required to undergo pre-election testing or IT audits and are not subject to the same procurement regulations as “voting systems”.

- Enterprise class technologies used in Florida elections include the voter registration system, automated signature verification, automated ballot duplication, mail assemblers and sorters, electronic poll books, election night reporting, and ballot tracking.
- The state selected the voter registration system, but it is minimally addressed in law.
- There are no controls in Florida’s laws for the rest of the enterprise-class technologies in use.
- Absent appropriate controls, these technologies can be compromised to prematurely expose election data, facilitate election fraud, and even change election outcomes.

2) Current state certification and pre-election testing standards for “voting systems” are outdated and manual cross-checks are needed to verify accuracy during the election.

- The published “voting system” certification manual was last updated in 2005.
- Voting systems have vulnerabilities to malware or bad actor access that can enable vote flipping, illegal ballot insertion, or deletion.
- Minimal hand counting is done to detect machine vote flipping or ballot manipulation.
- Procedures to detect bad actors scanning illegal ballots in off-hours are not specified.

3) Machine vote counting is mandated under current Florida law. There is no hand count option.

4) Extensive use of data network communications and USB thumb drives shared between “voting systems” and “other election systems” make all systems more vulnerable to malware, data breaches, and bad actor data manipulation.

- Cellular, wi-fi, and ethernet data communications are widely used in FL elections.
- Most systems utilize USB thumb drives which can be used to insert malware or steal data.

5) Florida is overly dependent on vendors and federal resources for technology expertise

- There is no requirement for any election system vendor or their personnel to be U. S. based.

Why the Election Technology Bill is the Only Real Solution

Goal	Election Technology Security Bill	President Trumps EO and Directives
Make “other election” systems secure	√	√
Manual cross-checks and audits for all election systems	√	TBD
Optional hand counting or machine counting of ballots	√	√ Required hand count
Minimize data network communications & secure portable data	√	TBD
Establish an election technology board, update certification standards, and conduct regular security risk assessments	√	TBD

For More Info: Technology Security Bill Rev 9-25 12pm