SUMMARY OF SOME TROUBLING PROVISIONS OF SB 22-153

A. It is bad policy to enact a statute knowing it contains conflicts with other existing statute. SB 22-153 creates such conflicts in at least two important respects.

   1. Section 10 of SB 22-153 requires all counties with populations over 1,000 to acquire and use electronic voting systems. No such provision exists in existing statute. However, existing statute, CRS 1-5-601.5, requires all electronic voting systems offered for sale in Colorado to comply with the voting system standards (VSS) promulgated by the Federal Election Commission in 2002. The first two forensic reports issued in the Tina Peters matter opined that the Mesa County system does not comply with the 2002 VSS in several respects. Virtually identical systems are used in 61 other Colorado Counties. It is likely that none of the systems in those counties comply with the 2002 VSS. Therefore, section 10 of SB 22-153 mandates that counties use illegal equipment. This is a direct conflict in statute that would be created by adoption of SB 22-153.

   2. Section 11 of SB 22-153 prohibits county officials, including the clerk and recorder, from making an image of the hard drive on a voting system. Existing statute, CRS 1-7-802, requires that the designated election official (typically the Clerk and Recorder of the county) preserve election records for at least 25 months after an election. USC sec. 20701 contains a similar requirement under federal law for a 22 month period. The affidavit of the election manager in Elbert County asserts that the secretary of state's representative admitted that the trusted build of the Dominion system would "wipe clean" the hard drive. This results in the destruction of election records. To discharge their statutory duties, county CCRs need to create and preserve copies of the hard drives to preserve election records that would be "wiped clean" by the trusted build or could be destroyed by other events. Section 11 of SB 22-153 is a direct conflict with the statutory duties of CCRs to preserve election records.

B. Electronic voting systems are "black box" systems that use opaque software to interpret, adjudicate, tabulate and report ballots and votes. No one in the Secretary of State's office, nor in any county clerk's office, knows how this is accomplished within the systems. No one other than the vendor can say whether the systems are reliable or whether they perform as expected by the voters. This has caused extensive lack of faith in election results. The solution is to make the systems more transparent and available to independent audit and review. Instead, this bill would create additional obstacles against transparency and further undermine public confidence in election results.

C. The bill would criminalize frivolous missteps by county clerks and yet leave the Secretary of State free from any criminal penalty for failing to perform her duties to ensure that the voting systems comply with state standards and perform reliably. It will disincentivize good people from seeking the office of county clerk and recorder out of fear of baseless and frivolous prosecution.

MORE COMMENTS ON WHY THIS IS A BAD BILL

Section 1-1-104 (1) Redefines “election records” by including key access card logs and security surveillance recordings. It omits to include logs on the computer systems that would indicate who has accessed the voting system, when, and to what purpose through electronic connectivities such as ethernet, wireless, and cellular. If the authors truly are concerned about system security, they should define election records to include any electronic record on the voting system.

Section 4 - Accelerates enforcement actions to be concluded within 30 days and <u>no right to appellate review</u> (review by Supreme Court is discretionary). Further, section 4 empowers the secretary of state to bring enforcement action without involvement of the attorney general. This eliminates an important potential brake on ill-advised actions by the secretary of state.

Section 5 - Allows Secretary of State or Coordinated Election Official to file verified petition for neglect of duty under CRS 1-1-113

Sections 6 and 7 - Require all election officials to be certified after indoctrination in courses provided by secretary of state. It overrides the county voters’ decisions by empowering the secretary of state veto power over the voters’ selection of chief election official for the county.

Section 8 - Criminalizes “knowingly false” statements by election officials that are critical of the administration of elections. While this section might appear harmless because it purports to punish only knowingly false statements, its effect would be to muffle critics of election system shortcomings through intimidation of prosecution.

Section 9 - Restricts access to voting equipment (making it a crime for unauthorized persons to enter the voting system room)

Section 10 - Requires every county to purchase and use electronic voting systems. Accordingly, if a county, such as Rio Blanco, loses faith in the electronic systems, they nevertheless would be required to use them and pay for them.

Section 11 - Forbids county personnel from making a backup image of the hard drive of any component of the voting system. This prohibits anyone knowledgeable of computer systems or voting systems to inspect and verify whether the systems, required in section 10 above, comply with state law. This also obstructs the statutory duty of county clerks and recorders to ensure that election records are retained for 25 months, as required by state statute.

Section 12 - Requires 24 hour video surveillance of voting systems

Section 13 - Allows secretary of state to overrule county canvass board's refusal to certify election results

Section 14 - Makes it a Class 1 Misdemeanor (penalty up to 18 months jail or $5,000 fine or both) to refuse to comply with rules or orders of the secretary of state

Section 15 - Makes it a Class 5 Felony (punishable by 1-2 years imprisonment and fine of up to $100,000) to (1) violate rules of SOS regarding access to voting systems, or (2) facilitate unauthorized access to voting system or election night reporting system, or (3) publish passwords or other confidential information relating to a voting system