

**Statement on Revised Draft
of Proposed Rules as issued**

May 18ⁿ, 2022

5/31/2022 comments by Harvie Branscomb (D) and Emily Brake (R)
[harvie \[at\] electionquality.com](mailto:harvie@electionquality.com) <http://electionquality.com>

(please do not redact the above contact information)

Transparency, verifiability, and access to accurate information about our elections are fundamental elements of trustworthy Colorado elections. We Coloradans deserve evidence-based elections.

Requested change in rulemaking process

Previous Secretaries of State released drafts of rules much sooner than has occurred in 2021 and 2022. They also published comments much sooner. By doing so they provided stakeholders a much more viable process for engagement prior to the highly regulated process of finalizing the rules. Increased participation and dialog during the drafting process favors a much less partisan and a more effective rulemaking process leading to fewer errors and contradictions in rules and greater clarity. Better engagement between voters and elections officials and public access to the evidence and information boosts confidence in our election processes and outcomes.

In the press release announcing the proposed rules, the Secretary of State's office wrote:

"All written comments will be posted online at the Department of State website: https://www.coloradosos.gov/pubs/rule_making/hearings/2022/ElectionsRulesHearing20220524.html. We will redact apparent personal contact information, including home address, email address, and telephone number(s), from submissions before posting the information online, unless otherwise directed by the contributor. All written comments will be added to the official rulemaking record."

While the SOS published an audio recording of the rule-making hearing, the rest of the expected publication of public comment is still missing and we understand that the written testimony will be published with the record of rulemaking. We would have preferred to have a chance to respond to other inputs to rulemaking as has been the case under previous office holders.

Upon review of recent instances of rulemaking over the past year, it was discovered that some written comments from organizations and parties were apparently held back from publication with other public comments. We hope to receive an explanation of any instances of redaction of entire comments from rulemaking. Likewise, we hope that in future rulemaking the Secretary will deem it appropriate to share the public comments at or near the time they are received.

We recommend for future consideration that election rules ought to include a provision for required publication of an inventory of election expertise at the Department of State. This publication would list the role of each election-applicable staff person (names for non-managing staff could be withheld) including the Secretary of State. Associated with each instantiated role would be a brief description of the practical election experience of the person in that role and dates of completion of the SOS approved certification training(s) for that person (if any). The dramatic extent of furtherance of dependence of elections administration on the staff of the Dept. of State, and particularly the decisions of the Secretary, that characterizes this unusual expansion of rules, makes such a publication almost essential. Voters

need to know the training and experience levels of those making powerful decisions previously under the control of local elections officials.

Requested rule change for pre-election cycle deadlines

Early voting in Colorado starts six weeks before Election Day. Many pre-Election Day election activities take place during this time frame as well, including but not limited to conducting Logic and Accuracy tests, training and hiring bipartisan citizen election judges, and most of all, addressing voter needs. It is a very busy time for election officials, watchers, candidates, ballot measure committees, and voters. Previous Secretaries of State worked hard to avoid adding greater burdens on limited resources during active election cycles. They avoided changing rules in the middle of active ballot issuance. They also did their best to ensure watcher certification and other trainings were up to date and commonly used forms were finalized prior to the start of early voting.

For the past few election cycles, there has been a chronic pattern of mid-election changes in rules, forms, trainings. Certification processes that were finalized after the start of early voting. Approvals on forms and other submitted to the Secretary of State are often delayed weeks, if not months, beyond the historical norm of prior office holders, sometimes well into early voting.

Meanwhile the Secretary of State in these proposed rules implements new and very short administrative deadlines on local officials, while not implementing any such standards upon the Secretary of State's administration itself. While there is a demand for local officials to act quickly, there is no such clear requirement on the Secretary of State to act timely, even when delays impact all of Colorado's sixty four counties that administer elections. Scrambling in the middle of election cycles to keep up with changes from the Secretary of State's office that could have been handled prior to the active election cycle increases the chances of error, confusion, and ineffective operations.

Ensuring rules, forms, certification trainings, and other ordinary elections administration responsibilities of the Secretary of State's office are finalized prior to the start of ballot issuance for early voting would increase effective engagement and improve confidence in elections.

We request the Secretary of State implement rules for the Dept of State to finalize non-emergent and commonly used forms, trainings, and election rules at least seven calendar days in advance of the start of early voting for an election.

Comments regarding proposed rules as drafted.

Note regarding formatting: To understand the inline commentary that follows, the rule text is in the original caps style font, our comments all begin at the left margin in Arial font. In earlier numbered sections the original rules that are not commented upon are redacted. In later sections, the entire rule remains in this text.

Inline comments by Harvie Branscomb (D) and Emily Brake (R).

General comments abstracted from the many details that follow:

1. This rule aligns too much with the deficient concept of "security by obscurity." Security through transparency of an evidence-based election is a far more appropriate and constructive concept, but absent here.

2. Instead the rule draft relies too much on complex perhaps impractical security processes required of local officials and requires reports only to the Secretary of State (SOS) without provisions for adequate public transparency.
3. The Colorado Secretary of State will not represent the interests of all Colorado voters better than the locally elected officials do. The concept of a multi-partisan state election board seems increasingly attractive as an alternative to vesting power in a single partisan statewide office
4. The Rule draft enables drastic sanctions (e.g. ends of careers in elections) for rules decided upon by a single partisan-elected individual who is subject to minimal oversight, with negligible compensatory opportunity for remedy or appeal other than through a distant future election.
5. This draft ironically fails to incorporate the benefits of Colorado's own Risk Limiting Audit (RLA), that when adequately implemented for multiple contests with sufficient public access to evidence and independence from original election judgments as well as contest selection decisions by the SOS. A properly implemented RLA will detect both errors and fraud to an extent adequate to escalate tabulation accuracy to what is needed. Colorado should instead recognize the unique and powerful value of the tabulation audit and write rules which leverage the lessened fear of incorrect outcomes that could be caused by interference with tabulation by insiders and outsiders.
6. This rule disparages independent evaluation of voting systems and may actually entirely obstruct such independent evaluations.
7. The large number of items that are to be reported to the SOS from local jurisdictions, but then not placed in the public domain, will result in a dramatic increase in periodic CORA requests to the SOS for these items, identified by the rule section that requires them. SOS can expect to see an increase in frequency of CORA requests and if the issue dates of these reports is unclear, expect multiple identical requests issued in an attempt to catch the reports on a timely basis. It would be more efficient and transparent to simply publish the reports automatically.

Original Rule Draft (portions removed) follows:

Disclaimer:

The proposed draft rules have changed. This draft supersedes the Preliminary Draft that was issued with the Notice of Proposed Rulemaking on April 15th, 2022. These revised proposed rules will be considered at the May 24th, 2022, rulemaking hearing.

~~26.4.21.1.16~~ "Continuing candidate" means a candidate who has not been eliminated but is not a winning candidate in a ranked voting election.

New Rule 1.1.17, concerning the definition of county throughout CCR 8 1505-1:

1.17 "COUNTY" OR "COUNTY CLERK" MEAN THE ELECTED COUNTY CLERK AS CHIEF ELECTION OFFICIAL FOR THE COUNTY, AND OTHERS EMPLOYED OR APPOINTED BY THE COUNTY CLERK TO CARRY OUT THE DUTIES OF THE COUNTY CLERK IN THE ADMINISTRATION OF AN ELECTION.

Assuming this definition has the scope of all election rules, the conflation of the personal role of County Clerk & Recorder (CCR) with the administrative role may be problematic. Employed "or appointed" implies that no employee agreement is needed and only designation is required (much like SB153 allows for the

SOS followup to canvass boards). This ironically weakens the “security” of the role of County Clerk & Recorder and could have unpredicted negative impacts on the security of our elections.

The Secretary of State in the reasoning for this change in definition, does not indicate sufficient reason and need for such a change that opens up a security risk to allow appointed non-deputized non-employee appointees to take on greater authority.

New Rule 1.1.29, concerning the definition of election project backup throughout CCR 8 1505-1:

1.1.29 “ELECTION PROJECT BACKUP” MEANS A SET OF FILES THAT IS GENERATED BY THE VOTING SYSTEM SOFTWARE’S DEDICATED BACKUP/EXPORT FUNCTIONS AND VENDOR DEFINED PROCEDURES AFTER THE INITIAL PROJECT IS CREATED THAT CAN BE USED TO RESTORE THE VOTING SYSTEM TO A PREVIOUS STATE. THIS DOES NOT INCLUDE A FULL OR PARTIAL HARD DRIVE IMAGE OR CLONE.

Elections belong to the citizens of Colorado. Elections processes should not be determined by unelected vendors. The concept of letting the vendor decide what data deserves to be backed up is contrary to the principle of security when one considers that any defects may have been inserted or left unintentionally by the vendor. Election errors or defects or deliberate malfeasance may be extant in the portion of data that is not backed up by the vendor designed backup functions. The SB153 concept to prevent anyone from cloning data or “imaging a drive” is nothing short of a very poorly thought out mistake that seems to be carried into rule here as well as elsewhere. While we support increasing the regular backing up of election management systems files, and maintaining the security of such backups, there must be means to also confirm the back up software from the vendor is working soundly and not limit backups to only what the vendor determines. Even when the voting system software is working correctly, to give such power to vendors to determine what will be backed up and saved, unnecessarily fuels distrust, not confidence, in Colorado elections.

New Rule 1.1.47:

1. “SECURE BALLOT AREA” MEANS:

A. ALL AREAS USED FOR PROCESSING BALLOTS, INCLUDING BUT NOT LIMITED TO:

1. SIGNATURE VERIFICATION;

1. BALLOT OPENING;

1. TABULATION; OR

1. STORAGE OF VOTED BALLOTS.

New Rule 1.1.48:

1. "SECURE EQUIPMENT AREA" MEANS:

A. ALL AREAS IN WHICH ELECTION MANAGEMENT EQUIPMENT IS USED, INCLUDING BUT NOT LIMITED TO:

1. PROGRAMMING;

1. COPYING ELECTION FILES TO OR FROM MEMORY CARDS OR FLASH MEDIA;

1. ADJUDICATING BALLOTS;

1. TALLYING RESULTS;

1. RESULTS REPORTING; OR

1. THE STORAGE AREA FOR ALL VOTING SYSTEM COMPONENTS.

This section should include areas used for ballot envelope sorter/scanning, Opex opening, and equipment used to process UOCAVAs and Txt2Cure

~~26.1.131.1.64~~ "Winning candidate" means a candidate who is elected after receiving at least **50 percent plus one vote** in an instant-run-off election, or after reaching the winning threshold required in a single transferrable vote election, or because the number of continuing candidates and other winning candidates is less than or equal to the number of seats to be filled.

The wording of this rule prompts us to jointly ask, "50 percent of what?" This must not be left unspecified, and should use the defined concept of "winning threshold". Ideally, the denominator should be all ballots legally cast containing the contest. IRV typically uses a much less obvious, less equitable definition namely 50 percent of the number of ballots left in the election that contain votes for continuing candidates plus one. If "winning threshold" is also applied to the IRV single winner case, then the correct denominator is the "total votes counted in the first round of tabulation" divided by 2 (the number of offices to be filled plus one). By using "votes counted" as opposed to "ballots cast" this formula arguably unfortunately still allows undervotes to be eliminated from the threshold calculation. This rule must be reworded.

~~26.1.141.1.65~~ "Winning threshold" means the number of votes sufficient for a candidate to be elected. In any given election, the winning threshold equals the total votes counted in the first round of tabulation, divided by the sum of one plus the number of offices to be filled, then adding one, disregarding any fractions. Winning threshold = $((\text{Total votes cast}) / (\text{Seats to be elected} + 1)) + 1$, with any fraction disregarded.

We request a change to the formula for “winning threshold.”

First, the winning threshold formula numerator should be “= (total votes counted)” not “(total votes cast),” Counted votes are usually less than cast votes or rather, cast ballots. Using total votes cast could mean the inclusion of votes on ballots not sent on for counting due to bipartisan election judges determining such ballots do not meet criteria to be counted. This happens every election due to some ballots missing signature on mail ballot affidavits.

Secondly, insufficient reasoning was given to justify lowering the typical winning threshold for the denominator to be $/(Seats\ to\ be\ elected + 1)$. Example: If 1000 votes are cast for a race with 4 seats, $1000/4$ plus 1 vote is usually what is used to determine the winning threshold, reflecting a formula of “Winning threshold = $((Total\ votes\ cast)/(Seats\ to\ be\ elected)) + 1$,”

Instead, using the formula as written in the drafted rule here, in this hypothetical race, the winning would be lower than typical, and in this case, would be $(1000/7)$ plus 1 vote. We propose this should be adjusted and changed to:

“Winning threshold = $((Total\ votes\ counted)/(Seats\ to\ be\ elected)) + 1$, with any fraction disregarded.”

Amendment to Rule 2.15.5, concerning a county’s custodianship over and distribution of non-resident voter information:

2.15.5 Custodianship of Voter Registration Information

a. The Secretary of State is the official custodian of the information contained in the centralized statewide registration system and the computerized statewide voter registration list created and maintained under section 1-2-301, C.R.S.

a. Each county clerk is the official custodian of the voter registration information only for electors within his or her THEIR county. IN THE EVENT THAT A COUNTY RECEIVES AN OPEN RECORDS REQUEST FOR A VOTER RECORD FOR AN ELECTOR OUTSIDE THEIR COUNTY, THEY MAY NOT PROVIDE THAT RECORD AS PART OF THE REQUEST AND MUST DIRECT THAT REQUESTOR TO SUBMIT THEIR REQUEST TO THE SECRETARY OF STATE’S OFFICE OR TO THE ELECTOR’S COUNTY OF RESIDENCE.

A. A COUNTY CLERK MAY NOT PROVIDE VOTER RECORD INFORMATION OUT OF SCORE UNLESS:

1. THE INFORMATION WAS REQUESTED UNDER PART 21, ARTICLE 72 OF TITLE 24, C.R.S., FOR AN ELECTOR WITHIN THEIR COUNTY; OR

1. THE COUNTY IS OTHERWISE REQUIRED BY LAW TO PROVIDE THAT INFORMATION.

This section confirms a trend to restrict transparency- not only to prevent access for an elector “outside their county” – that really ought to be described as a residence address in another county- but it also much more drastically restricts access to data to flow only through the Colorado Open Records Act (CORA), which is to implement a mechanism that is deliberately inconvenient and often suffers from unnecessary costs and obstacles. Harvie Branscomb usually asks officials to provide data outside of CORA if they choose. Other election watchers obtain per election rules and as affirmed allowable by the Secretary of State’s own watcher certification training, a rolling list of voters who have cast ballots.

The language in this rule change may prevent that very polite and efficient approach working with local officials. There is much information within SCORE that is not “for an elector” or watcher, and in fact refers to ballot styles, and other protected personally identifiable information. This rule is inadequate to serve the purpose of CORA. Also Harvie Branscomb and others have repeatedly been told that SOS has no authority over CORA, yet here is an attempt to be involved in changing Colorado Open Records Act policy.

This rule does not address voters that are in multiple counties, such as those that have a landowners ballot in one county or reside in one county but have a mailing address in another. It creates issues for proper administration of municipal and school and special elections that include multiple counties or elections that use SCORE data but are not overseen by the State..

The Secretary of State’s Office (SOS) is currently behind schedule on the administrative tasks it has already taken on and away from county administration. SOS watcher trainings are out of date and processing of many routine election matters is chronically delayed. For the most practical purposes, placing more tasks on this office will add to further delays, which will lead to further lack of transparency, further lack of provision of information, and the side effects will fuel distrust.

There is insufficient grounds given for this rule change to justify implementation.

New Rule 6.9, concerning a county informing the Colorado Department of State that an election judge is removed from their duties:

6.9 THE COUNTY MUST IMMEDIATELY INFORM THE SECRETARY OF STATE’S OFFICE IN WRITING IN THE EVENT THAT AN ELECTION JUDGE IS REMOVED FROM DUTY BY THE COUNTY

This seems unnecessary and inefficient for county officials. On the other hand it does mean that the SOS becomes the central custodian of a CORA-able record of election judge dismissals and that may be a convenience to those who are researching election problems. Being able to monitor if there are large removals of election judges may point to a need for further investigation and election watcher oversight in a particular area of an election process. At the same time, citizen poll workers are concerned about what additional information may be released along with a removal being reported to the Secretary of State. For example, they are concerned about their health privacy needs not being appropriately addressed, such as in the case of a judge being removed due to death or illness. The change cannot be supported in it’s current wording. It does not appropriately limit the information that may be released both to the SOS and public. The Dept of State should engage further discussion on this issue with election judges, Clerks & Recorders, election watchers monitoring elections, and Colorado voters before implementation of such a policy. .

Amendment to Rule 8.8, pertaining to watchers and ballot drop boxes:

8.8 The minimum number of watchers the county clerk must accommodate for each appointing entity is as follows:

[No changes to Rules 8.8.1 through 8.8.3.]

8.8.4 AT EACH BALLOT DROP BOX, ONE WATCHER.

Certified watchers representing candidates, parties, ballot measure committees maintaining full access to every step in election activity (except for voters making a mark on a ballot) is important for building and keeping confidence in election outcomes.

This rule also creates an impossible standard for counties to meet. Rule 8.7.1 establishes “The County Clerk must provide, and identify in some manner, at least one primary contact for watchers at each location where election activities are performed when watchers are present.”

Does the SOS intend for there to be staffing at every drop off box for watcher check in? If not, the rules will need to be remedied and addressed appropriately.

[Not shown current Rule 8.8.4 renumbered to 8.8.5.]

Amendments to Rule 8.10.2 concerning watchers and their duties:

1. Watchers must be permitted access that would allow them to attest to the accuracy of election-related activities. This includes personal visual access at a reasonable proximity to read documents, writings or electronic screens and reasonable proximity to hear election-related discussions between election judges and electors.

a. Election activities include:

(12) BALLOT PRINTING AND MAILING PREPARATION THAT OCCUR AT THE COUNTY CLERK’S OFFICE.

What is the reason that applicable election activities occur only at the county clerk’s office when obviously ballot printing and mailing preparation outside the clerk’s office deserve just as much attention if not more? Numerous errors have historically been inserted into Colorado elections by commercial entities operating outside of county offices where oversight is minimal or nonexistent.

A. INDIVIDUALS ALLOWED TO ATTEND THE LOGIC AND ACCURACY TEST UNDER SECTION 1- 7-509(2), C.R.S., DO NOT NEED TO BE CREDENTIALLED AS WATCHERS. THE COUNTY

CLERK MAY LIMIT ATTENDANCE TO THE LOGIC AND ACCURACY TEST SUBJECT TO SPACE LIMITATIONS AND LOCAL SAFETY CODES.

It is inappropriate to think that of all the election activities, only the LAT is allowable to the public and everything else requires appointment by SOS or by interested parties, subject to dismissal by the county clerk. The case for broader, nonpartisan observation has also been made at *How More Robust Election Observation Could Help Save U.S. Elections – Alliance For Securing Democracy* <https://securingdemocracy.gmfus.org/how-more-robust-election-observation-could-help-save-u-s-elections/> Surely a gold standard state would allow public access to other election activities to build voter confidence in election results.

Our request is to allow public access to the Risk Limiting Audit (RLA). Public access to RLA has been available in most counties and it’s been helpful to build confidence in elections. Withdrawing the RLA from a list of

publicly accessible election events can only diminish its effectiveness. The RLA is meant largely to satisfy the public, not just the officials who manage it.

Repeal of current Rules 11.1.1 and 11.1.2:

1. ~~The designated election official must securely store election setup records. Only persons with the clerk's written authorization may access the records.~~

1. ~~The county clerk must deputize employees who are authorized to prepare or maintain the voting system or election setup records before the election.~~

Direct evidence of loss of local control, which is the significant downside of Colorado's modernization of elections. Not enough cause or reason has been given to need to change the rules to eliminate rule 11.1.1 and 11.1.2.

New Rule 11.4, pertaining to election database project backups:

1. ELECTION DATABASE PROJECT BACKUPS

1. IF THE COUNTY'S VOTING SYSTEM DOES NOT EXPORT LOGS FROM THE ELECTION MANAGEMENT SYSTEM WHEN AN ELECTION PROJECT BACKUP IS CREATED, THE COUNTY MUST ALSO EXPORT THE LOGS FROM THE ELECTION MANAGEMENT SYSTEM FOR RETENTION ACCORDING TO RULE 20.10.2 AT THE TIME THEY CREATE AN ELECTION PROJECT BACKUP ACCORDING TO THE PROCEDURES DEFINED BY THE VOTING SYSTEM VENDOR.

This paragraph remains vague about what logs are to be backed up. The EMS for the Dominion system might exist in several servers (RTR, Adjudication, etc.) and this paragraph does not make clear what devices are subject to backup. Also it does not make clear what logs are required to be backed up nor is it clear that the procedures defined by the voting system vendor are adequate to serve the purposes of the law. Likewise the previous requirement to "backup" after various events may not be specific enough to result in an adequate backup of data, particularly in light of the drastic restriction to prevent backup by "image", the simplest method that guarantees broad coverage of the backup. We speak to this issue from a volume of experience in technology, including Harvie Brancomb's experience as a vendor for software to create image back ups and Emily Brake's experience in data accounting and security.

We support the Election Security position of the League of Women Voters of Colorado (<https://bit.ly/LWVCOElectionSecurity>), which calls for public access to the source code of election systems and samples of election equipment. If that would compromise the security of the voting system, the voting system should be fixed.

New Rule 11.4.3, recodified from Rule 11.4. Rules 11.4.1 through 11.4.6 re-codified under subsections (a) through (f). Grammatical changes to subsection (b):

- 11.4.11.4.3 A county that electronically tabulates election results must submit election setup records to the Secretary of State so that they are received no later than 5:00 p.m. on the seventh day before election day.

This timing is inappropriate as scanning may have been underway for 7 days prior to this date. Request this rule be changed to state “no later than 5pm on the day before scanning may begin.” Otherwise this rule change creates more doubt, not more confidence, in our elections.

11.4.6(F) All parties must treat as confidential all escrowed materials and any other related information that comes into their possession, control, or custody.

This strangely broad statement would appear to attempt to obstruct CORA access almost completely.

Escrow agreements between vendors and the government should be open for oversight and review. Voters are the most significant stakeholder in our elections and they should not be shut out via attempts to reduce their rights under CORA.

Amendment to 11.7.3 (b) concerning a cross-reference change:

a. If the malfunction requires a programming or election setup change to the database or other parts of the voting system, the designated election official must submit an updated election setup record to the Secretary of State’s office as set forth in ~~Rule 11.4.~~RULE 11.4.3.

Amendment to Rule 15.1.4, concerning the review of petition entries:

15.1.4 Verifying individual entries

[Not shown: no changes to subsections (a) through (d).]

(e) Secretary of State or DEO staff will not use any of the following discrepancies as the sole reason to reject an entry:

[Not shown: no changes to sub-subsections (1) through (7).]

(8) On a signer line, the date is missing but a line above ~~or~~ AND below has an acceptable date; or

[Not shown: no changes to sub-subsection (9).]

[Not shown: repeal of current Rule 20 to re-codify security rules throughout 8 CCR 1505-1 to New Rule 20, clarify and update existing rules, and reorganize overall structure.]

New Rule 20, concerning the security procedures for counties:

New Rule 20.1, concerning security plans and the proposed permanent adoption of New Rule 20.6.2 (part of which is re-organized as Rule 20.1.2(e) for clarity) and amendments to Rule 20.7 (part of which is re-organized as Rule 20.1.2(f) for clarity) that were temporarily adopted on February 10, 2022:

1. SECURITY PLAN

1. THE COUNTY MUST SUBMIT ITS SECURITY PLAN ON THE FORM PRESCRIBED BY THE SECRETARY OF STATE IN ACCORDANCE WITH SECTION 1-5-616(5), C.R.S., NOT LESS THAN 60 DAYS BEFORE AN ELECTION. A COUNTY MAY AMEND ITS SECURITY PLAN WITHIN 60 DAYS OF AN ELECTION AS A RESULT OF AN UNFORESEEN CIRCUMSTANCE. THE COUNTY MUST DOCUMENT THE CHANGES AND FILE THE REVISIONS WITH THE SECRETARY OF STATE WITHIN FIVE DAYS OF THE CHANGE.

The status of the security plan with respect to CORA must be clarified for the sake of confidence in elections processes. If there are portions of the security plan that for some reason must remain obscure, please call these out in the rules and have these portions segregated for easy redaction upon open records request so that the public can be informed about the security of its election. The election plan, the watcher plan, and the security plans for the state should be under the custodianship of the Dept of State (who designs the format and requires production of the data) but the format must be supportive of the need for appropriate public access.

1. IN THE SECURITY PLAN, THE COUNTY MUST PROVIDE THE FOLLOWING INFORMATION:

A. SAMPLE COPIES OF ALL SECURITY FORMS, SCHEDULES, LOGS, AND CHECKLISTS THEY WILL USE IN THE UPCOMING ELECTION;

A. DETAILED PLANS REGARDING THE TRANSPORTATION OF EQUIPMENT AND BALLOTS TO REMOTE VOTING SITES AND BACK TO THE CENTRAL ELECTIONS OFFICE OR STORAGE FACILITY;

A. THE DETAILS OF THE SECURITY TRAINING IT WILL PROVIDE, INCLUDING THE TIME, LOCATION, AND NUMBER OF ELECTION OFFICIALS RECEIVING THE TRAINING, IN ACCORDANCE WITH RULE 20.3;

A. THE NAME, TITLE, AND DATE A BACKGROUND CHECK WAS CONDUCTED FOR EACH EMPLOYEE FOR WHOM THE COUNTY CLERK IS REQUIRED TO PERFORM A BACKGROUND CHECK UNDER RULE 20.2.3;

A. ALL VOTING SYSTEM ACCEPTABLE USE POLICY AGREEMENTS SIGNED BY COUNTY STAFF WHICH HAD NOT PREVIOUSLY BEEN PROVIDED IN A SECURITY PLAN THAT CALENDAR YEAR;

A. A DESCRIPTION OF THE ENVIRONMENT IN WHICH VOTING SYSTEM COMPONENTS WILL BE KEPT IN ACCORDANCE WITH RULE 20.5.5; AND

A. ANY OTHER INFORMATION REQUIRED IN THE PUBLISHED SECURITY PLAN.

New Rule 20.2, regarding background checks:

1. BACKGROUND CHECKS

1. BACKGROUND CHECKS GENERALLY

A. A PERSON MAY NOT ACCESS THE SYSTEMS, INFORMATION, OR AREAS OUTLINED IN THIS RULE UNTIL A BACKGROUND CHECK OF THAT PERSON HAS BEEN PERFORMED AND PASSED.

“A person” is too non-specific. This rule is extremely vague and has inappropriate universal scope- to the effect that neither the public nor credentialed watchers will be able to access information without encountering gatekeeping for which there is no obvious arrangement for passage. What does “systems, information or areas outlined in this Rule” actually mean? Could it be read to mean any or all information about the election? The background check itself remains vague – are the criteria for passage exactly no conviction for fraud or conviction for election offense (no matter how long ago, etc.)? The phrase “a person may not access” is too broad to be commensurate with the rest of the rule section that refers to staff and vendors and election judges. A more appropriate intro might be “An election official or official designee of an election official, including employees of vendors may not be given access...”.

Additionally, without better clarification this rule opens the door to confusion about whether the SOS is seeking a requirement of background checks of watchers, who only watch those who access the system. It suggests a possibility of a return of background check requirements for watchers without indicating the process and means for this, including who will pay for such background checks. Watchers ability to witness and verify elections must be preserved. Consider rewording this section to better to affirm the right of watchers to watch all election activities in full.

A. A BACKGROUND CHECK THAT IS REQUIRED BY THIS RULE MUST BE RUN AT LEAST ONCE PER CALENDAR YEAR, PRIOR TO THE FIRST ELECTION OF THE YEAR. IN A YEAR IN WHICH A PRESIDENTIAL PRIMARY WILL BE HELD, THE BACKGROUND CHECK MAY BE PERFORMED IN DECEMBER IN THE YEAR PRIOR TO THE PRESIDENTIAL PRIMARY.

A. UNLESS OTHERWISE NOTED, A BACKGROUND CHECK REQUIRED BY THIS RULE MUST BE REQUESTED FROM THE COLORADO BUREAU OF INVESTIGATION.

B. A BACKGROUND CHECK MAY ONLY BE CONSIDERED TO HAVE PASSED IF THE CHECK FINDS THAT THE PERSON HAS NOT BEEN CONVICTED OF:

1. AN ELECTION OFFENSE; OR

1. AN OFFENSE WITH AN ELEMENT OF FRAUD.

1. THE COUNTY CLERK MUST PERFORM A BACKGROUND CHECK IN ACCORDANCE WITH THIS RULE FOR EACH ELECTION JUDGE IF THE JUDGE REQUIRES ACCESS TO:

A. THE STATEWIDE VOTER REGISTRATION DATABASE;

A. ELECTOR'S CONFIDENTIAL OR PERSONALLY IDENTIFIABLE INFORMATION; OR

The definition of "election official" in Title 1 of state law is:

(10) "Election official" means any county clerk and recorder, election judge, member of a canvassing board, member of a board of county commissioners, member or secretary of a board of directors authorized to conduct public elections, representative of a governing body, or other person contracting for or engaged in the performance of election duties as required by this code.

Current election rules also state: :

1.1.33 "Personally identifiable information" means information about an individual that can be used to distinguish or trace an individual's identity, such as an elector's social security number, driver's license number, email address, month and day of birth, and signature.

Personally identifiable information or PII is defined but still is insufficiently clear for use in such a requirement for a background check and needs to be better defined. The term "elector's confidential" in the proposed rule 20.2.2 is not at all defined. Either allows discretionary interpretation that might differ between the county and the SOS and others. This may be especially true in light of the new normal of extremely competitive or argumentative disparity between state and some county officials. To avoid such issues, what voter information is shareable with the public and what information is not public and requires a background check to access needs to be better defined.

A. VOTER REGISTRATION APPLICATIONS OR OTHER LIST MAINTENANCE ACTIVITIES.

1. THE COUNTY CLERK MUST PERFORM A BACKGROUND CHECK IN ACCORDANCE WITH THIS RULE FOR EACH PERMANENT OR TEMPORARY STAFF MEMBER WITH ACCESS TO:

A. THE STATEWIDE VOTER REGISTRATION DATABASE;

A. ELECTOR'S CONFIDENTIAL OR PERSONALLY IDENTIFIABLE INFORMATION;

A. VOTER REGISTRATION APPLICATIONS OR OTHER LIST MAINTENANCE ACTIVITIES;

A. A COMPONENT OF THE COUNTY'S VOTING SYSTEM WHILE AT A LOCATION OR DURING TRANSPORT;

A. REMOVABLE MEDIA THAT CONTAINS AN ELECTION PROJECT BACKUP; OR

A. A CODE, LOCK, COMBINATION, PASSWORD, OR ENCRYPTION KEY FOR:

1. VOTING EQUIPMENT;

 1. BALLOT STORAGE AREA;

 1. COUNTING ROOM;

 1. LOCATION OF ADJUDICATION WORKSTATIONS; OR

 1. LOCATION OF TABULATION WORKSTATION.
-
1. A VOTING SYSTEM PROVIDER MUST ARRANGE FOR A BACKGROUND CHECK, SUFFICIENT TO DETERMINE IF THE INDIVIDUAL HAS EVER BEEN CONVICTED OF AN ELECTION OFFENSE OR AN OFFENSE WITH AN ELEMENT OF FRAUD FOR EACH EMPLOYEE OR CONTRACTOR WHO CONDUCTS WORK ON ANY COMPONENT OF A COUNTY'S VOTING SYSTEM. THE PROVIDER MUST AFFIRM THAT THE CHECK WAS CONDUCTED IN WRITING TO THE SECRETARY OF STATE PRIOR TO THE EMPLOYEE CONDUCTING ANY WORK.

 1. THE DEPARTMENT OF STATE MUST PERFORM A CRIMINAL BACKGROUND CHECK FOR EACH STAFF MEMBER WHO CONDUCTS WORK ON ANY COMPONENT OF A COUNTY'S VOTING SYSTEM PRIOR TO CONDUCTING THAT WORK.

The Colorado Department of State staff, and all persons, should be under the same requirements as election judges, county staff, vendors, all others. There should not be a carve-out for some of the Secretary of State's administrative staff to be convicted of election offenses and/or fraud, and unlike all others, still be able to work on any component of a county's voting system. We request the use of the same equitable standard for all. It is better to clarify that "staff" here includes but is not limited to Colorado Department of State staff. "Persons" would be more appropriate and would include all election officials including election judges.

New Rule 20.3, pertaining to security training:

1. SECURITY TRAINING

1. THE COUNTY MUST CONDUCT SECURITY TRAINING FOR ALL ELECTION-RELATED FIELD TECHNICIANS, ELECTION-RELATED CONTRACTORS, AND ELECTION OFFICIALS.

Access to adequate training is foundational. We request that access to security training be expanded beyond what is defined as an election official to watchers, political party officials, and if so desired, the general public.

1. THE SECURITY TRAINING REQUIRED BY THIS RULE MUST INCLUDE THE FOLLOWING COMPONENTS:

A. PROPER APPLICATION AND VERIFICATION OF SEALS AND CHAIN-OF-CUSTODY LOGS;

A. HOW TO DETECT TAMPERING WITH VOTING EQUIPMENT, MEMORY CARDS, OR ELECTION DATA ON THE PART OF ANYONE COMING IN CONTACT WITH VOTING EQUIPMENT, INCLUDING ELECTION OFFICIALS, VENDOR PERSONNEL, OR VOTERS;

A. ENSURING PRIVACY IN VOTING BOOTHS;

A. CHAIN-OF-CUSTODY REQUIREMENTS FOR VOTING EQUIPMENT, ACTIVATION CARDS, AND OTHER ELECTION MATERIALS;

A. BALLOT SECURITY;

A. VOTER ANONYMITY; AND

“Voter anonymity” is not defined or declared in Colorado regulations. The Address Confidentiality Program (ACP) is an important program for which there should be greater education for the public on how it functions for the limited population of voters it serves. ACP provides a service approaching “voter anonymity” and should be specifically named if that is what is sought.

However, the section on voter anonymity should be changed to refer to ballot anonymity (or as it is too often called, “ballot secrecy” even though ballots are not secrets.)

Please also add the following: “ballot and ballot envelope handling equipment” to the list in order to provide for proper security of envelope scanner sorters and devices that manage and perform signature verification.

Please add “ensuring voter confidence through evidence-based transparency” to teach all parties engaged in managing and overseeing elections that a major component of security is transparent and verifiable access to an evidence-based election.

A. RECOGNITION AND REPORTING OF SECURITY INCIDENTS.

New Rule 20.4, pertaining to physical security. Proposed permanent adoption of amendments to Rule 20.5.3(a) (re-organized New Rule 20.4.1(b) and amended for clarity):

1. PHYSICAL SECURITY

1. REQUIREMENTS FOR CODES, LOCKS, AND COMBINATIONS

A. THE COUNTY MUST MAINTAIN RESTRICTED ACCESS TO SECURE BALLOT AREAS AND SECURE EQUIPMENT AREAS AS DEFINED BY RULES 1.1.47 AND 1.1.48, BY USE OF A CODE, LOCK, OR OTHER COMBINATION. THIS MAY INCLUDE THE USE OF A KEY CARD ACCESS SYSTEM WHICH ALSO LOGS ENTRY INTO THE SECURE AREA.

A. THE COUNTY CLERK MAY ONLY GIVE THE CODE, LOCK, OR COMBINATION REQUIRED BY THIS RULE TO EMPLOYEES WHO HAVE PASSED A BACKGROUND CHECK IN ACCORDANCE WITH RULE 20.2.

A. THE COUNTY MUST CHANGE THE CODE, LOCK, OR COMBINATION REQUIRED BY THIS RULE AT LEAST ONCE PER CALENDAR YEAR PRIOR TO THE FIRST ELECTION OF THE YEAR.

1. SURVEILLANCE OF SECURE AREAS

Access to camera technology is mixed. Some counties have reported supply chain issues in securing equipment. Harvie Branscomb has seen in a small county an election staff member assigned to hold up a cell phone as a camera to satisfy the previous incantation of this rule at least during the time he was present as a watcher. It would be wise to be aware of any inability of the counties to fulfill this very valuable rule, considering their real world situation. Also there is no point in recording all this video data unless it is actually accessible for review later. These rules must also be paired with easy access to the security videos. CORA requests to access the video should not be met with fees outside of reasonable affordability.

Experience with attempts to access such video data suggests that too often it is not available, was never properly implemented, is too costly to obtain, or is unstructured so as to be impossible to learn anything from it. Please be wise about such costly projects when the video will be saved for later review.

Video that is streamed to the internet is a much more valuable resource because the public can notice the events and items that might require a later review. Brake observed both sides of the broadcast of video of a Risk Limiting Audit for a large county and it was very helpful for citizen oversight and thus the building of trust in that elections process. Any video that is captured should (really must) include audio because much more information is gleaned from the world of sound in conjunction with picture. Anything found within streams and recordings that might act as an obstacle to public access (either if streamed or post facto by CORA request) should be designed not to be included, or redacted at the cost of the custodian.

A. THE COUNTY MUST MAKE VIDEO SECURITY SURVEILLANCE RECORDINGS OF SECURE EQUIPMENT AREAS AS DEFINED BY RULE 1.1.48, EXCLUDING VOTING BOOTHS, BEGINNING AT LEAST 60 DAYS BEFORE

ELECTION DAY AND CONTINUING THROUGH AT LEAST 30 DAYS AFTER ELECTION DAY. IF A RECOUNT OR CONTEST OCCURS, THE RECORDING MUST CONTINUE THROUGH THE CONCLUSION OF ALL RELATED ACTIVITY.

A. THE COUNTY MUST ALSO MAKE VIDEO SECURITY SURVEILLANCE RECORDINGS OF SECURE BALLOT AREAS AS DEFINED BY RULE 1.1.47, EXCLUDING VOTING BOOTHS,

BEGINNING AT LEAST 35 DAYS BEFORE ELECTION DAY AND CONTINUING THROUGH AT LEAST 30 DAYS AFTER ELECTION DAY. IF A RECOUNT OR CONTEST OCCURS, THE RECORDING MUST CONTINUE THROUGH THE CONCLUSION OF ALL RELATED ACTIVITY.

A. THE VIDEO SECURITY SURVEILLANCE RECORDING SYSTEM MUST:

1. ENSURE THAT RECORDS ARE NOT WRITTEN OVER WHEN THE SYSTEM IS FULL;
1. PROVIDE A METHOD TO TRANSFER THE VIDEO RECORDS TO A DIFFERENT RECORDING DEVICE OR TO REPLACE THE RECORDING MEDIA; AND
1. IF REPLACEABLE MEDIA IS USED, PROVIDE A PROCESS THAT ENSURES THAT THE MEDIA IS REPLACED OFTEN ENOUGH TO PREVENT PERIODS WHEN RECORDING IS NOT AVAILABLE.

A. THE COUNTY MUST ADEQUATELY LIGHT THE AREAS SUBJECT TO VIDEO SURVEILLANCE IN THIS RULE TO PROVIDE VISIBILITY FOR VIDEO RECORDING.

Proposed permanent adoption of amendments to current Rule 20.6.1(h) (re-organized within Rule 20.4.3, amended into subsections for clarity) temporarily adopted on February 10, 2022:

1. ACCESS LOGS TO SECURE AREAS

A. THE COUNTY MUST MAINTAIN A LOG OF EACH PERSON WHO ENTERS A SECURE BALLOT AREA AS DEFINED BY RULE 1.1.47 OR SECURE EQUIPMENT AREA AS DEFINED BY RULE 1.1.48.

A. A LOG REQUIRED UNDER THIS RULE MUST CONTAIN THE:

1. NAME OF THE PERSON ACCESSING THE AREA; AND
1. YEAR, MONTH, DAY, HOUR, MINUTE, AND WHETHER THE TIME IS A.M. OR P.M. THAT THE AREA WAS ACCESSED.

A paper record log is a public record accessible under CORA, and a digital record should be as well.

While only the automated key card access is required to be printed on paper, presumably all such logs will be saved on paper.

If the "minute" is to be recorded one must assume that the minute of arrival and also the minute of departure will be recorded, and yet in at least some counties, it is not recorded. With most key card systems, it can be the case that only one person in a group accompanying the key card holder is adequately logged. In practice, others will often walk in with that person or the doors propped open on a regular basis.

If this rule is to be seriously executed, greater attention will be needed to record names of persons entering these areas and ensure all the persons either complete a paper log or each and every time they enter an exit, they use a key card.

Such logs must include each and every election judge, watcher, SOS observers, vendors and anyone else entering and exiting.

A. IF A LOG IS GENERATED BY USE OF A KEY CARD OR SIMILAR DOOR ACCESS SYSTEM, THAT SYSTEM MUST BE CAPABLE OF PRODUCING A PRINTED PAPER LOG THAT MEETS THE REQUIREMENTS OF THIS RULE.

Proposed permanent adoption of amendments to current Rule 20.5.3(a), (c), and (d) (re-organized within New Rule 20.4.4(a), amended into sub-subsections for clarity) and temporary New Rule 20.5.3(b) (re-organized as Rule 20.4.4(c)) that were temporarily adopted on February 10, 2022:

1. RESTRICTIONS ON PHYSICAL ACCESS

Nothing in elections should be done alone for the protection of all involved. While these restrictions on access are well intended and adequately drafted, there is no complementary arrangement for avoidance of authorized staff to be present alone as unique individuals unmonitored by anyone else. The rule ought to exclude any such individual access and arrange for any access to the protected area to be combined with adequately published rules for access for watchers. To make these rules serious about security, transparency must also be considered and assured.

A. GENERAL RESTRICTIONS

1. NO PERSON MAY BE PRESENT IN A SECURE BALLOT AREA AS DEFINED BY RULE 1.1.47 OR SECURE EQUIPMENT AREA AS DEFINED BY RULE 1.1.48 UNLESS:

A. THEY ARE EMPLOYEES AUTHORIZED TO HAVE A CODE, LOCK, OR COMBINATION TO THE AREA UNDER RULE 20.4.1;

A. THEY ARE SUPERVISED BY EMPLOYEES AUTHORIZED TO ACCESS THAT AREA; OR

B. THEY ARE EMERGENCY PERSONNEL RESPONDING TO AN EMERGENCY SITUATION. IN THE EVENT EMERGENCY PERSONNEL ACCESS THIS AREA WITHOUT SUPERVISION, THE COUNTY MUST IMMEDIATELY INFORM THE DEPARTMENT OF STATE.

1. IN EXTREME CIRCUMSTANCES, THE COUNTY MAY REQUEST, AND THE SECRETARY OF STATE MAY GRANT, AN EXEMPTION FROM THE REQUIREMENTS OF THIS RULE.

A. INDIVIDUALS DELIVERING BALLOTS BETWEEN SEPARATE ROOMS MUST WEAR DISTINGUISHING IDENTIFICATION.

Ballots means also ballot envelopes or ballot packets.

A. ANY INDIVIDUAL WHO IS PROHIBITED FROM HAVING PHYSICAL CONTACT WITH ANY VOTING EQUIPMENT UNDER SECTION 1-5-607(1), C.R.S. MAY NOT ACCESS A ROOM WITH VOTING EQUIPMENT UNLESS ACCOMPANIED BY ONE OR MORE INDIVIDUALS WITH AUTHORIZED ACCESS.

This should be scoped to limit access to the Secure Equipment Area and not just "any individual who is prohibited..."

There should be a separate enabling rule that requires access by watchers if there is one or more individuals in a Secure Equipment Area or a Secure Ballot Area. Please change the first sentence as follows:

(B) **"No individual (authorized or otherwise) may access a secure equipment area or secure ballot area unless accompanied by one or more individuals with authorized access."**

That is an adequate and in fact strong security rule. No individuals alone may have access.

1. REMEDIES

A. IN THE EVENT THAT A COUNTY DISCOVERS THAT A VIOLATION OF RULE 20.4 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.4.

The rule cited in the above sentence is voluminous and a massive expansion of SOS role.

We have a system of government that works best with checks and balances. A government entity, any entity, deciding it can take "any action" is usually struck down by courts for cause. Insufficient reasons

have been provided for these rule changes that would give the SOS unique and groundbreaking level of power to take “any action” it chooses to do in response to an alleged violation of law.

If the SOS is intending to limit any action to only certain types of actions then this should be more clearly stated.

Additionally, we hope that similar remedies will be provided for the same level of action to be possible to remedy the failure to provide adequate oversight to credentialed watchers and to the public, where appropriate. Otherwise this rule is irresponsibly one-sided and retrograde in effect. It is counter to often advertised maintenance of a “gold standard” elections in Colorado.

New Rule 20.5 concerning the security of voting systems and including the proposed permanent adoption of amendments to current Rule 20.4.1(re-organized as New Rule 20.5.1(a)) that were temporarily adopted on February 10, 2022:

1. SECURITY OF VOTING SYSTEM

1. CHAIN-OF-CUSTODY REQUIREMENTS

A. COUNTY CLERKS MUST CONTINUOUSLY COMPLY WITH THE SEAL REQUIREMENTS OF THE MOST RECENT CONDITIONS OF USE ISSUED BY THE SECRETARY OF STATE FOR THE COUNTY’S VOTING SYSTEM. COUNTY CLERKS MAY NOT ALLOW ANY UNATTENDED VOTING SYSTEM COMPONENT TO REMAIN UNSEALED AT ANY POINT AFTER TRUSTED BUILD HAS BEEN INSTALLED ON A COMPONENT.

Conditions of use are available to the public once promulgated (deeply hidden within the voting systems pages of the SOS site) but are not as far as one can tell subject to any public review. It is not as public as even this drafted rule. Drafted rule 20.5.1 should be reworded to provide better public access and involvement in all regulatory processes and material that relate to registration database, eligibility and tabulation systems.

A. THE COUNTY MUST MAINTAIN AND DOCUMENT UNINTERRUPTED CHAIN-OF-CUSTODY FOR EACH VOTING SYSTEM COMPONENT FROM THE INSTALLATION OF TRUSTED BUILD TO THE PRESENT, THROUGHOUT THE COUNTY’S OWNERSHIP OR LEASING OF THE DEVICE.

A. TO MAINTAIN UNINTERRUPTED CHAIN-OF-CUSTODY FOR EACH VOTING SYSTEM COMPONENT THE COUNTY MUST:

1. RECORD THE SERIAL NUMBER OF EVERY SEAL REQUIRED BY THE CONDITIONS OF USE ON THE APPROPRIATE CHAIN-OF-CUSTODY LOG; AND

1. WHEN REMOVING OR REPLACING SEALS, USE TWO ELECTION OFFICIALS TO VERIFY, AND INDICATE BY SIGNING AND DATING THE LOG, THAT THE SEAL SERIAL NUMBERS MATCH THE LOGGED SERIAL NUMBERS. THE ELECTION OFFICIALS SHOULD BE OF DIFFERENT PARTY AFFILIATIONS WHENEVER POSSIBLE.

Nothing in elections should be done alone or done by one party only. It sets up election officials to be at greater risk of accusations of misconduct when they are permitted to do things alone or attended by those of a single political party. Exceptions should be made only in extreme and rare situations. It is requested that “whenever possible” is struck from the rule.

New Rule 20.5.2, including the proposed permanent adoption of New Rule 20.6.2 (re-organized as New Rule 20.5.2(a), amended to sub-subsections for clarity) and amendments to current Rules 20.5.4(a) (re-organized as New Rule 20.5.2(b)) and 20.6.1 (re-organized as New Rule 20.5.2(c)) that were temporarily adopted on February 10, 2022:

1. ACCESSING THE VOTING SYSTEM

This section is hindered by the limitations of the definition of “voting system” that avoids inclusion of the systems that conduct signature verification and manage signature verification and other steps of eligibility determination.

A. ACCEPTABLE USE POLICY AGREEMENT

1. ALL USERS WITH ACCESS TO THE VOTING SYSTEM MUST SIGN THE VOTING SYSTEM ACCEPTABLE USE POLICY AGREEMENT PROVIDED BY THE SECRETARY OF STATE EVERY YEAR PRIOR TO USING THE SYSTEM.
1. THE COUNTY CLERK MUST SUBMIT COPIES OF ALL NEWLY SIGNED ACCEPTABLE USE POLICY AGREEMENTS SIGNED BY ELECTION STAFF WITH THE COUNTY’S SECURITY PLAN.

A. EXCEPT FOR VOTERS USING A VOTING SYSTEM COMPONENT TO VOTE DURING AN ELECTION, COUNTY CLERKS MAY NOT ALLOW ANY PERSON TO ACCESS ANY COMPONENT, INCLUDING THE HARD DRIVE(S) OR COPIES OF ANY PART OF THE HARD DRIVE(S) FOR ANY COMPONENT, OF A COUNTY’S VOTING SYSTEM UNLESS:

1. THAT PERSON HAS PASSED THE BACKGROUND CHECK REQUIRED BY THIS OR ANY OTHER RULE OR LAW; AND
1. THAT PERSON IS PERFORMING A TASK PERMITTED BY THE COUNTY CLERK OR THE SECRETARY OF STATE THAT IS PERMITTED BY STATUTE OR RULE, AND IS:

A. AN EMPLOYEE OF THE COUNTY CLERK;

A. APPOINTED AS AN ELECTION JUDGE BY THE COUNTY CLERK IN ACCORDANCE WITH ARTICLE 6 OF TITLE 1, C.R.S.;

A. AN EMPLOYEE OF THE VOTING SYSTEM PROVIDER FOR THE COUNTY'S VOTING SYSTEM; OR

A. AN EMPLOYEE OR DESIGNEE OF THE SECRETARY OF STATE.

This is the rule that would obstruct if not prevent an appropriate expert from performing constructive election research. It would have prevented Harvie Branscomb from performing clerk-permitted research on voting systems in Eagle County several decades ago. Because that research demonstrated critical fallibility of vote counting, the systems were replaced by modern equipment at that time. Ensuring appropriate vetted experts are able to conduct research on how we can better secure elections is foundational to building better elections.

There is no reference to the text of the "Acceptable Use Policy" that is contemplated. Since agreement to that policy is pivotal to getting access to both work on and study the systems, the policy should be published in draft form and made subject to the rulemaking process.

A. ACCOUNTS AND PASSWORDS

1. THE COUNTY CLERK MUST CHANGE ALL PASSWORDS ASSOCIATED WITH A VOTING SYSTEM ACCORDING TO THE SCHEDULE REQUIRED BY THE MOST RECENT CONDITIONS OF USE FOR THAT VOTING SYSTEM.
1. THE COUNTY CLERK MAY USE THE ADMINISTRATIVE USER ACCOUNT FOR THE ELECTION MANAGEMENT SYSTEM ONLY TO CREATE INDIVIDUAL USER ACCOUNTS FOR EACH ELECTION PROJECT.
1. THE COUNTY CLERK MUST CREATE INDIVIDUAL USER ACCOUNTS THAT ARE ASSOCIATED AND IDENTIFIED WITH EACH INDIVIDUAL AUTHORIZED USER OF THE OPERATING SYSTEM OF THE VOTING SYSTEM, ELECTION MANAGEMENT SYSTEM, OR ELECTION PROJECT.
1. THE COUNTY CLERK MUST RESTRICT ACCESS TO EACH INDIVIDUAL USER ACCOUNT WITH A UNIQUE PASSWORD KNOWN ONLY TO EACH INDIVIDUAL USER.

AUTHORIZED USERS MUST ACCESS THE OPERATING SYSTEM OF THE VOTING SYSTEM, ELECTION MANAGEMENT SYSTEM, AND ELECTION

PROJECT USING HIS OR HER INDIVIDUAL USER ACCOUNT AND UNIQUE PASSWORD.

1. THE COUNTY CLERK MAY GRANT ADMINISTRATIVE PRIVILEGES TO NO MORE THAN FOUR INDIVIDUAL USER ACCOUNTS PER ELECTION UNLESS THE COUNTY HAS REQUESTED AND BEEN AUTHORIZED BY THE SECRETARY OF STATE TO GRANT MORE. THE COUNTY MUST IDENTIFY THE EMPLOYEES WITH ADMINISTRATIVE PRIVILEGES IN THE SECURITY PLAN FILED WITH THE SECRETARY OF STATE.

1. THE COUNTY CLERK MAY ONLY GRANT ADMINISTRATIVE PRIVILEGES FOR THE OPERATING SYSTEM OF THE VOTING SYSTEM TO THE COUNTY CLERK, EMPLOYEES OF THE COUNTY, AND ANY PERSON APPOINTED BY THE SECRETARY OF STATE TO ASSIST IN THE ADMINISTRATION OF AN ELECTION, SUBJECT TO THE RESTRICTIONS OF RULE 20.5.2(c)(9). THE COUNTY CLERK MAY ONLY GRANT ADMINISTRATIVE PRIVILEGES TO THE ELECTION MANAGEMENT SYSTEM OR THE ELECTION PROJECT TO THE COUNTY CLERK, EMPLOYEES OF THE COUNTY CLERK'S OFFICE, AND ANY PERSON APPOINTED BY THE SECRETARY OF STATE TO ASSIST IN THE ADMINISTRATION OF AN ELECTION, SUBJECT TO THE RESTRICTIONS OF RULE 20.5.2(c)(9).

1. AUTHORIZED USERS WITH ADMINISTRATIVE PRIVILEGES OF THE OPERATING SYSTEM, ELECTION MANAGEMENT SYSTEM, OR ELECTION PROJECT MAY NOT SHARE THEIR ACCOUNTS OR PASSWORDS WITH ANYONE.

1. THE COUNTY CLERK MUST DISABLE ALL ACCOUNTS TO ACCESS THE OPERATING SYSTEM FOR INDIVIDUALS WHO ARE NO LONGER EMPLOYED BY THE COUNTY OR ARE NO LONGER EMPLOYED IN A ROLE THAT REQUIRES ACCESS TO THE VOTING SYSTEM.

1. ANY INDIVIDUAL WHO IS PROHIBITED FROM HAVING PHYSICAL CONTACT WITH ANY VOTING EQUIPMENT UNDER SECTION 1-5-607(1), C.R.S. MAY NOT GRANT THEMSELVES OR BE GRANTED WITH AN ACCOUNT OR PASSWORD FOR THE OPERATING SYSTEM OF THE VOTING SYSTEM, THE ELECTION MANAGEMENT SYSTEM, OR AN ELECTION PROJECT.

1. THE VOTING SYSTEM PROVIDER MAY NOT HAVE ADMINISTRATIVE OR USER ACCESS TO THE COUNTY'S ELECTION MANAGEMENT SYSTEM.

1. THE CIVIL SERVANTS AT THE DEPARTMENT OF STATE WILL MAINTAIN ALL BIOS PASSWORDS FOR VOTING SYSTEM COMPONENTS.

A. IN ADDITION TO THE AUDIT LOGS GENERATED BY THE ELECTION MANAGEMENT SYSTEM, THE COUNTY MUST MAINTAIN CONTEMPORANEOUS MANUAL ACCESS LOGS

THAT ACCURATELY RECORD THE DATE, TIME, AND USER'S NAME, AND PURPOSE FOR EACH INSTANCE THAT A USER ENTERS OR EXITS THE SYSTEM.

New Rule 20.5.3, including the proposed permanent adoption of amendments to current Rule 20.6.1(e) (re-organized as New Rule 20.5.3(a)(1)), temporary New Rule 20.6.1(g) (re-organized as New Rule 20.5.3(a)(2)), current temporary Rule 20.6.1(d) (re-organized as New Rule 20.5.3(b)(2)), amendments to current Rule 20.6.1(f) (re-organized as New Rule 20.5.3(b)(3)), and amendments to current Rule 20.6.4 (re-organized as New Rule 20.5.3(c)) that were temporarily adopted on February 10, 2022:

1. CONNECTING TO THE VOTING SYSTEM

0. SYSTEM SETTINGS

1. IF ANY COMPONENT OF THE VOTING SYSTEM IS EQUIPPED WITH WI-FI CAPABILITY OR A WIRELESS DEVICE, THE COUNTY CLERK MUST ENSURE THAT THE WIRELESS CAPABILITY OR DEVICE IS DISABLED BEFORE USE IN AN ELECTION.

This lacks clarity whether the disabling is in hardware or software. Obviously disabling the hardware is the most secure remedy.

1. THE COUNTY CLERK MAY NOT ALTER, OR GRANT PERMISSION TO ANYONE ELSE TO ALTER, EXCEPT DURING THE TRUSTED BUILD PROCESS, THE PRE-BOOT SETTINGS FOR ANY VOTING SYSTEM COMPONENT, INCLUDING ALTERING THE BOOT PATH.

A. EXTERNAL NETWORK CONNECTION FORBIDDEN

1. THE COUNTY CLERK MUST USE THE VOTING SYSTEM ONLY ON A CLOSED NETWORK OR IN A STANDALONE FASHION.

Here the limitation on meaning of "voting system" takes on some importance as eligibility systems are often connected to the internet. From the current Election Rules, the definition:

"Voting system" as defined in section 1-1-104(50.8), C.R.S., means:

(a) The total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used to:

- (1) Define ballots;
 - (2) Cast and count votes;
 - (3) Report or display election results; and
 - (4) Maintain and produce any audit trail information.
- (b) The practices and associated documentation used to:
- (1) Identify system components and versions of such components;
 - (2) Test the system during its development and maintenance;
 - (3) Maintain records of system errors and defects;
 - (4) Determine specific system changes to be made to a system after the

initial qualification of the system; and

(5) Make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

(c) "Voting system" does not include any other component of election administration, such as voter registration applications or systems, electronic pollbooks, ballot delivery and retrieval systems, signature verification and envelope sorting devices, ballot on demand printers, election night reporting and other election reporting systems, and other components used throughout the election process that do not capture and tabulate votes.

Note that some of these elements of the definition may in practice be connected to internet in common practice.

1. THE COUNTY CLERK MAY NOT CONNECT OR ALLOW A CONNECTION OF ANY VOTING SYSTEM COMPONENT TO THE INTERNET.

1. THE COUNTY CLERK MAY NOT CONNECT ANY COMPONENT OF THE VOTING SYSTEM TO ANOTHER DEVICE BY MODEM.

A. REMOVABLE STORAGE DEVICE

1. THE COUNTY CLERK MUST REFORMAT ALL REMOVABLE STORAGE DEVICES IMMEDIATELY BEFORE CONNECTING THEM TO ANY COMPONENT OF THE VOTING SYSTEM, EXCEPT AS PROVIDED IN RULE 20.5.3(C)(2)-(5), OR IN THE CONDITIONS OF USE.

1. THE COUNTY CLERK MAY CONNECT TO THE ELECTION MANAGEMENT SYSTEM, WITHOUT FIRST REFORMATTING, A REMOVABLE STORAGE DEVICE CONTAINING ONLY ELECTION DEFINITION DATA FILES DOWNLOADED FROM SCORE IF:

A. THE COUNTY CLERK REFORMATS THE REMOVABLE STORAGE DEVICE IMMEDIATELY BEFORE INSERTING IT INTO THE SCORE WORKSTATION AND DOWNLOADING THE ELECTION DEFINITION DATA FILES; AND

A. BEFORE AND WHILE DOWNLOADING THE SCORE ELECTION DEFINITION DATA, THE COUNTY CLERK INSTALLS AND OPERATES THE ADVANCED NETWORK MONITORING AND THREAT DETECTION APPLICATIONS PROVIDED OR APPROVED BY THE SECRETARY OF STATE.

1. THE COUNTY CLERK MAY INSERT, WITHOUT FIRST REFORMATTING, A REMOVABLE STORAGE DEVICE INTO A BMD, IF:

A. THE REMOVABLE STORAGE DEVICE CONTAINS ONLY ELECTION AND BALLOT STYLE DATA FILES NECESSARY TO PROGRAM THE BMD FOR TESTING OR USE IN AN ELECTION;

A. THE COUNTY CLERK DOWNLOADED THE ELECTION AND BALLOT STYLE DATA FILES DIRECTLY FROM THE ELECTION MANAGEMENT SYSTEM WORKSTATION;

B. THE COUNTY CLERK DID NOT EXPOSE THE REMOVABLE STORAGE DEVICE TO THE INTERNET OR INSERT IT INTO AN INTERNET-CONNECTED DEVICE AFTER DOWNLOADING THE ELECTION AND BALLOT STYLE DATA FILES FROM THE ELECTION MANAGEMENT SYSTEM; AND

A. THE COUNTY CLERK REFORMATTED THE REMOVABLE STORAGE DEVICE IMMEDIATELY BEFORE INSERTING IT INTO THE ELECTION MANAGEMENT SYSTEM AND DOWNLOADING THE ELECTION AND BALLOT STYLE DATA FILES.

1. THE COUNTY MAY INSERT A REMOVABLE STORAGE DEVICE INTO THE ELECTION MANAGEMENT SYSTEM, WITHOUT FIRST REFORMATTING IT IF THE REMOVABLE STORAGE DEVICE CONTAINS ONLY ELECTION DATABASE OR PROJECT FILES REMOTELY PROGRAMMED BY THE VOTING SYSTEM PROVIDER IN ACCORDANCE WITH RULE 20.8.1.

1. THE COUNTY CLERK MAY INSERT A REMOVABLE STORAGE DEVICE INTO THE ELECTION MANAGEMENT SYSTEM WITHOUT FIRST REFORMATTING IT IF THE REMOVABLE STORAGE DEVICE CONTAINS ONLY ELECTION DATABASE BACKUP

FILES CREATED BY THE COUNTY AND:

A. THE COUNTY CLERK SUBMITS AN ATTACHMENT WITH THEIR SECURITY PLAN STATING SECURITY PROCEDURES FOR THE REMOVABLE STORAGE DEVICE THAT ADDRESSES STORAGE OF THE DEVICE WHEN NOT IN USE; AND

A. THE PLAN IN THE ATTACHMENT IS APPROVED BY THE SECRETARY OF STATE.

A. THE COUNTY MAY NOT INSTALL ANY SOFTWARE ON ANY COMPONENT OF THE VOTING SYSTEM UNLESS DIRECTED TO, OR APPROVED BY, THE DEPARTMENT OF STATE.

A. ACTIVATION CARDS

1. THE COUNTY MUST ASSIGN AND SECURELY AFFIX A PERMANENT UNIQUE IDENTIFIER TO EACH REMOVABLE CARD OR ACTIVATION CARD. THE COUNTY MAY USE THE MANUFACTURER ASSIGNED SERIAL NUMBER FOR THIS PURPOSE.

1. THE COUNTY MUST HANDLE ACTIVATION CARDS IN A SECURE MANNER AT ALL TIMES.
THE COUNTY MUST TRANSFER AND STORE ANY CARD OR ACTIVATION CARD IN A SECURE CONTAINER WITH AT LEAST ONE SEAL. UPON DELIVERY AND RECEIPT, ELECTION JUDGES OR COUNTY PERSONNEL MUST VERIFY, AND INDICATE BY SIGNING AND DATING THE CHAIN-OF CUSTODY LOG, THAT ALL SEAL NUMBERS MATCH THOSE LISTED IN THE LOG.

1. THE COUNTY MUST MAINTAIN A WRITTEN OR ELECTRONIC LOG TO RECORD ACTIVATION CARD SEALS AND TRACK SEALS FOR EACH VOTING UNIT.

1. THE COUNTY MUST MAINTAIN A COMPLETE INVENTORY OF ACTIVATION CARDS, INCLUDING WHICH VSPC THEY ARE ASSIGNED TO DURING AN ELECTION. BEFORE AND AFTER A VSPC OPENS AND CLOSES EACH DAY, THE SUPERVISOR JUDGE MUST VERIFY THAT ALL CARDS ISSUED TO THE VSPC ARE PRESENT. IF AT ANY TIME THE SUPERVISOR JUDGE CANNOT ACCOUNT FOR ALL ACTIVATION CARDS ISSUED TO THE VSPC, THE SUPERVISOR JUDGE OR A MEMBER OF THE

COUNTY ELECTION STAFF MUST IMMEDIATELY SUBMIT AN INCIDENT REPORT TO THE SECRETARY OF STATE UNDER RULE 11.7.

A. NO PERSON MAY MANUALLY CONNECT ANYTHING TO A VOTING SYSTEM COMPONENT THAT ENABLES A WIRELESS CONNECTION. THIS INCLUDES, BUT IS NOT LIMITED TO, EXTERNAL OR ADDITIONAL NETWORK INTERFACE CARDS, OTHER WIRELESS ANTENNAS, OR USB MICE OR KEYBOARDS THAT UTILIZE WIRELESS COMMUNICATION.

1. TRANSPORTING VOTING SYSTEM

A. THE COUNTY MUST SUBMIT DETAILED PLANS TO THE SECRETARY OF STATE BEFORE AN ELECTION REGARDING THE TRANSPORTATION OF VOTING SYSTEM COMPONENTS BOTH TO REMOTE VOTING SITES AND BACK TO THE CENTRAL ELECTIONS OFFICE OR STORAGE FACILITY.

A. DURING OR AFTER TRANSPORTATION, IF THERE IS ANY EVIDENCE OF POSSIBLE TAMPERING WITH A SEAL, OR IF THE SEAL NUMBERS DO NOT MATCH THOSE LISTED IN THE CHAIN-OF-CUSTODY LOG, THE COUNTY CLERK MUST BE IMMEDIATELY NOTIFIED AND MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. TRANSPORTATION BY COUNTY PERSONNEL

1. COUNTY PERSONNEL MUST AT ALL TIMES DISPLAY IDENTIFICATION PROVIDED BY THE COUNTY.

1. TWO EMPLOYEE SIGNATURES AND DATE ARE REQUIRED AT THE DEPARTURE LOCATION VERIFYING THAT THE EQUIPMENT IS SEALED TO DETECT TAMPERING. UPON DELIVERY OF EQUIPMENT, AT LEAST TWO ELECTION OFFICIALS MUST VERIFY, AND INDICATE BY SIGNING AND DATING THE CHAIN-OF-CUSTODY LOG, THAT ALL SEALS ARE INTACT AND THAT THE SEAL NUMBERS MATCH THE LOGGED SEAL NUMBERS.

A. TRANSPORTATION BY ELECTION JUDGES

1. TWO ELECTION JUDGES OF DIFFERENT PARTY AFFILIATIONS THAT ARE RECEIVING OR TRANSPORTING EQUIPMENT MUST INSPECT ALL VOTING DEVICES AND VERIFY THE SPECIFIC SEAL NUMBERS BY SIGNATURE AND DATE ON THE CHAIN-OF-CUSTODY LOG FOR THE DEVICE.

A. TRANSPORTATION BY CONTRACT

1. IF A COUNTY CONTRACTS FOR THE DELIVERY OF EQUIPMENT TO REMOTE VOTING LOCATIONS, EACH INDIVIDUAL DELIVERING EQUIPMENT MUST SUCCESSFULLY PASS A CRIMINAL BACKGROUND CHECK AS REQUIRED BY RULE 20.2.1.

1. TWO ELECTION OFFICIALS MUST VERIFY THE SPECIFIC SEAL NUMBERS BY DEVICE, SIGN, AND DATE THE CHAIN-OF-CUSTODY LOG UPON RELEASE OF THE EQUIPMENT TO THE INDIVIDUALS DELIVERING THE EQUIPMENT. UPON DELIVERY OF EQUIPMENT, AT LEAST TWO ELECTION OFFICIALS MUST VERIFY, AND INDICATE BY SIGNING AND DATING THE CHAIN-OF-CUSTODY LOG, THAT ALL SEALS ARE INTACT AND THAT THE SEAL NUMBERS MATCH THE LOGGED SEAL NUMBERS.

1. A COUNTY MUST REQUIRE A CONTRACTOR TO DELIVER EQUIPMENT TO A REMOTE LOCATION ON THE DAY THE EQUIPMENT IS PICKED UP.

New Rule 20.5.5, including the proposed permanent adoption of amendments to current Rule 20.7 (re-organized as New Rule 20.5.5, separated and amended into subsections (a) and (b) for clarity) that were temporarily adopted on February 10, 2022:

1. STORAGE OF VOTING SYSTEM

A. THE COUNTY CLERK MUST KEEP ALL COMPONENTS OF THE VOTING SYSTEM IN A LOCATION WITH LOGS AND ACCESS CONTROLS REQUIRED BY RULE 20.4.

A. THE COUNTY CLERK MUST KEEP ALL COMPONENTS OF A VOTING SYSTEM IN A TEMPERATURE-CONTROLLED STORAGE ENVIRONMENT THAT:

1. MAINTAINS A MINIMUM TEMPERATURE OF 50 DEGREES FAHRENHEIT AND A MAXIMUM TEMPERATURE OF 90 DEGREES FAHRENHEIT; AND

1. IS DRY WITH STORAGE AT LEAST FOUR INCHES ABOVE THE FLOOR.

1. RETENTION OF VOTING EQUIPMENT

A. IF A COUNTY RETAINS VOTING SYSTEM EQUIPMENT AFTER THE TERMINATION OF A LICENSE AGREEMENT WITH A VENDOR, THE COUNTY MUST REFORMAT ANY OF THOSE VOTING SYSTEM COMPONENTS AS DIRECTED BY THE SECRETARY OF STATE, AND THE COUNTY MAY NOT:

1. USE THE EQUIPMENT FOR ANY OTHER PURPOSE UNTIL THE COMPONENTS HAVE BEEN REFORMATTED; OR

1. TRANSFER THE EQUIPMENT TO ANY OTHER DEPARTMENT WITHIN THE COUNTY OR ANY PARTY OUTSIDE THE COUNTY UNTIL THE COMPUTERS HAVE BEEN REFORMATTED.

A. ALL SECURITY STANDARDS IN THIS RULE 20 ARE STILL APPLICABLE TO VOTING SYSTEM EQUIPMENT UNTIL THE COMPONENTS HAVE BEEN REFORMATTED.

A. BEFORE THE COMPONENTS ARE REFORMATTED, THE COUNTY MUST PRESERVE ALL ELECTION RECORDS REQUIRED TO BE PRESERVED BY RULE 20 FOUND ON THE VOTING SYSTEM.

A. THESE REQUIREMENTS ALSO APPLY TO ANY EQUIPMENT THAT A COUNTY NO LONGER USES AS VOTING SYSTEM EQUIPMENT BUT RETAINS WHILE A LICENSE AGREEMENT WITH A VENDOR IS IN FORCE.

New Rule 20.5.7, concerning the leasing of voting equipment by other jurisdictions:

1. USE OF VOTING EQUIPMENT BY OTHER JURISDICTIONS

A. A COUNTY MAY NOT TRANSFER ANY ELECTION EQUIPMENT TO ANY MUNICIPALITY, SPECIAL DISTRICT, OR ANOTHER LOCAL JURISDICTION, EXCEPT TO ANOTHER COUNTY CLERK AND RECORDER.

This level of distrust of both equipment and the local officials is damaging to election confidence and suggests that our local jurisdictions are untrustworthy and that our tabulation audit is insufficient to detect and deter error and fraud involving voting systems. It has been common practice to transfer election equipment to other election jurisdictions both within and outside the state. There are various needs for access to election equipment for testing purposes that involve no reason to result in a deleterious effect on Colorado's election integrity. Much of these new rules represent arduous requirements with little positive and probably negative effect. We must support municipal, special, and other elections better to help increase confidence in their results and not leave them in a position of scraping by with technology that is hard to secure and/or outdated.

A. IF A COUNTY TRANSFERS ANY ELECTION EQUIPMENT TO ANOTHER COUNTY WITHIN THE STATE, THE COUNTY RECEIVING THE EQUIPMENT MUST FOLLOW ALL SECURITY

PROCEDURES FOR THAT EQUIPMENT REQUIRED BY STATUTE OR THESE RULES THROUGHOUT THE TIME THE RECEIVING COUNTY HAS CUSTODY OF THE EQUIPMENT.

A. A COUNTY WHO IS TRANSFERRING ELECTION EQUIPMENT TO ANOTHER COUNTY MUST NOTIFY THE SECRETARY OF STATE OF THE TRANSFER BY FILLING OUT AN ACQUISITION/DISPOSITION FORM AND TRANSMITTING IT TO THE SECRETARY OF STATE. THE FORM MUST BE FILLED OUT AT BOTH THE TIME OF THE TRANSFER TO AND TRANSFER FROM THE COUNTY RECEIVING THE EQUIPMENT.

New Rule 20.5.8, including the proposed permanent adoption of temporary New Rule 20.15.3 (re-organized as New Rule 20.5.8(b)) that was temporarily adopted on February 10, 2022:

1. REMEDIES

A. GENERALLY

1. IN THE EVENT THAT A COUNTY DISCOVERS THAT A VIOLATION OF RULE 20.5 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

1. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.5.

A. IN THE EVENT THAT AN ELECTION OFFICIAL KNOWS, OR REASONABLY SHOULD KNOW, THAT THE COUNTY'S VOTING SYSTEM WAS ACCESSED BY ANY INDIVIDUAL NOT PERMITTED ACCESS BY THESE RULES OR IS MADE AWARE THAT THE

SYSTEM HAS BEEN TAMPERED WITH, THEY MUST IMMEDIATELY NOTIFY THE SECRETARY OF STATE.

New Rule 20.6, regarding trusted build procedures and including the proposed permanent adoption of temporary New Rule 20.20 (re-organized as New Rule 20.6) that was temporarily adopted on February 10, 2022:

1. TRUSTED BUILD PROCEDURES

1. WHEN TRUSTED BUILD REQUIRED

A. IN THE EVENT THAT THE SECRETARY OF STATE DETERMINES A TRUSTED BUILD IS REQUIRED IN A COUNTY, INCLUDING DUE TO A NEW CERTIFICATION, MODIFICATION, OR OTHER SECURITY ISSUE, THE COUNTY CLERK AND VOTING SYSTEM PROVIDER MUST COORDINATE WITH THE SECRETARY OF STATE TO INSTALL TRUSTED BUILD ON A SCHEDULE DETERMINED BY THE SECRETARY OF STATE'S OFFICE.

A. AT THE TIME THAT THE SECRETARY OF STATE DETERMINES A TRUSTED BUILD IS REQUIRED, THE SECRETARY OF STATE WILL PROVIDE THE REASON TO THE COUNTY CLERK FOR THE REQUIRED TRUSTED BUILD.

1. ATTENDANCE AT TRUSTED BUILD

(A) THE ONLY INDIVIDUALS WHO MAY BE PRESENT AT A TRUSTED BUILD IN A COUNTY INCLUDE:

- (1) SECRETARY OF STATE STAFF, DESIGNEES OF THE SECRETARY OF STATE, OR OTHER INDIVIDUALS APPROVED BY THE SECRETARY OF STATE;
- (2) VOTING SYSTEM VENDOR STAFF FOR THE VOTING SYSTEM FOR WHICH TRUSTED BUILD IS BEING INSTALLED; AND

1. THE COUNTY CLERK, EMPLOYEES OF THE COUNTY CLERK, OR THE DESIGNATED ELECTION OFFICIAL OF THE COUNTY, AS LONG AS THOSE INDIVIDUALS ARE AUTHORIZED TO ACCESS THE VOTING SYSTEM UNDER RULE 20.5.2(b) HAVE SIGNED THE VOTING SYSTEM ACCEPTABLE USE POLICY AGREEMENT, AND SUBJECT TO THE RESTRICTIONS OF RULE 20.4.4(c).

A. THE COUNTY CLERK AND VOTING SYSTEM VENDOR MUST PROVIDE THE NAME AND POSITION OF INDIVIDUALS WHO WILL ATTEND THE TRUSTED BUILD IN A COUNTY AT THE TIME OF SCHEDULING THE TRUSTED BUILD WITH THE SECRETARY OF STATE.

A. BACKGROUND CHECK

1. ANY INDIVIDUAL PRESENT AT THE TRUSTED BUILD MUST HAVE HAD A BACKGROUND CHECK CONDUCTED IN ACCORDANCE WITH RULE 20.2.

1. THE COUNTY CLERK AND VOTING SYSTEM VENDOR MUST PROVIDE PROOF THAT A BACKGROUND CHECK WAS CONDUCTED AND PASSED ON INDIVIDUALS WHO WILL BE PRESENT TO THE SECRETARY OF STATE AT THE TIME OF SCHEDULING THE TRUSTED BUILD WITH THE SECRETARY OF STATE'S OFFICE.

A. THE COUNTY CLERK AND VOTING SYSTEM VENDOR MAY ONLY ALLOW THE NUMBER OF PEOPLE DESIGNATED BY THE SECRETARY OF STATE FOR THAT COUNTY TO ATTEND THE TRUSTED BUILD.

A. IF, DUE TO AN UNFORESEEN CIRCUMSTANCE, THE COUNTY CLERK OR VOTING SYSTEM VENDOR MUST SEND AN INDIVIDUAL NOT PREVIOUSLY IDENTIFIED TO THE TRUSTED BUILD, THE COUNTY CLERK OR VENDOR MUST IMMEDIATELY CONTACT THE SECRETARY OF STATE AND PROVIDE THE INFORMATION OTHERWISE REQUIRED BY THIS RULE TO THE SECRETARY OF STATE FOR THE SUBSTITUTE INDIVIDUAL.

1. SECURITY AT TRUSTED BUILD

A. THE COUNTY CLERK MUST ENSURE THAT THE LOCATION WHERE THE TRUSTED BUILD WILL BE CONDUCTED DOES NOT ALLOW FOR INDIVIDUALS WHO ARE NOT PERMITTED TO ATTEND TO BE PRESENT OR TO OTHERWISE DISRUPT THE TRUSTED BUILD PROCESS.

A. VIDEO SURVEILLANCE RECORDING

1. THE COUNTY CLERK MUST ENSURE THAT THE TRUSTED BUILD IS CONDUCTED UNDER VIDEO SURVEILLANCE AS DEFINED BY RULE 1.1.60.

1. THE COUNTY CLERK MUST IDENTIFY THE VIDEO SURVEILLANCE EQUIPMENT THAT WILL BE USED TO COMPLY WITH THIS RULE TO THOSE ATTENDING THE TRUSTED BUILD.

1. VIDEO SURVEILLANCE OF THE TRUSTED BUILD MUST BE MAINTAINED AS AN ELECTION RECORD UNDER SECTION 1-7-802, C.R.S.

1. NO ONE MAY SURREPTITIOUSLY RECORD THE TRUSTED BUILD BY VIDEO OR AUDIO.

All of 20.6 reflects a failing principle of security through obscurity and confusion for the public when the opposite is what is needed. If this rule were written with the intention to maximize election confidence through evidence-basis and public understanding, it would require streaming video and audio of the trusted build with a substantial public education program about the need for and advantages to be obtained from the change of election software. At a bare minimum, election judges or watchers could be provided access to observe this election process to help restore confidence. There is no viable reason given as to why the trusted build needs to be done in virtual or actual secrecy.

1. COMPLETION OF TRUSTED BUILD

- A. COUNTY CLERKS MUST SEAL ALL VOTING SYSTEM COMPONENTS IN ACCORDANCE WITH THE MOST RECENT CONDITIONS OF USE ISSUED BY THE SECRETARY OF STATE FOR THE

- COUNTY'S VOTING SYSTEM IMMEDIATELY UPON CONCLUSION OF THE TRUSTED BUILD UNLESS THE COUNTY CLERK PROCEEDS TO AND COMPLETES ACCEPTANCE TESTING ON THE SAME DAY THAT TRUSTED BUILD IS COMPLETED.

- A. IN THE EVENT THAT THE CONDITIONS OF RULE 20.6.4(A) ARE MET, A COUNTY MUST SEAL ALL VOTING SYSTEM COMPONENTS IN ACCORDANCE WITH THE MOST RECENT CONDITIONS OF USE ISSUED BY THE SECRETARY OF STATE FOR THE COUNTY'S VOTING SYSTEM UPON CONCLUSION OF THE ACCEPTANCE TESTING.

- A. THE COUNTY CLERK MUST SUBMIT A COPY OF THE SIGNED TRUSTED BUILD AFFIDAVIT TO THE SECRETARY OF STATE FOLLOWING THE COMPLETION OF ACCEPTANCE TESTING.

1. IN THE EVENT THAT A TRUSTED BUILD CANNOT BE SCHEDULED OR COMPLETED DUE TO A COUNTY CLERK'S VIOLATION OF THESE RULES OR IN THE EVENT THAT A COUNTY CLERK IS FOUND TO HAVE VIOLATED THESE RULES FOLLOWING A TRUSTED BUILD, THE SECRETARY OF STATE MAY TAKE ANY OF THE ACTIONS LISTED IN RULE 20.12.2(B).

Another example of asymmetric authority being concentrated into a single statewide official and use of "any action" to establish overly broad power in one office without adequate checks and balances. This may fuel greater partisanship in elections administration and must be adjusted to a more limited standard.

New Rule 20.7, pertaining to the security of ballots:

1. SECURITY OF BALLOTS

1. UNVOTED BALLOTS

- A. THE COUNTY MUST SECURE UNVOTED PAPER BALLOTS DURING PRE-ELECTION STORAGE, TRANSPORTATION, AND AT POLLING LOCATIONS.

1. EXCEPT WHEN ELECTION JUDGES ARE ACTIVELY ISSUING BALLOTS THE BALLOT CONTAINERS MUST BE SEALED.

1. THE COUNTY MUST MAINTAIN CHAIN-OF-CUSTODY LOGS FOR ALL BALLOT CONTAINERS.

A. UNVOTED PAPER BALLOTS MUST BE TRANSPORTED TO POLLING LOCATIONS IN SEALED CONTAINERS. THE COUNTY CLERK MUST RECORD THE SEAL NUMBER ON A CHAIN-OF-CUSTODY LOG FOR VERIFICATION BY THE RECEIVING ELECTION JUDGES. THE RECEIVING ELECTION JUDGES MUST VERIFY THE BALLOT CONTAINER SEAL NUMBER BEFORE ISSUING BALLOTS.

A. WHEN ELECTION JUDGES ARE ACTIVELY ISSUING BALLOTS, THE UNVOTED BALLOTS MUST BE IN CLEAR VIEW OF A MINIMUM OF TWO ELECTION JUDGES OF DIFFERENT PARTY AFFILIATIONS AND ONE OF THE ELECTION JUDGES MUST ACTIVELY MONITOR THE BALLOTS UNLESS THE BALLOTS ARE STORED IN A LOCKED LOCATION ACCESSIBLE ONLY TO ELECTION OFFICIALS.

A. A MINIMUM OF TWO ELECTION JUDGES OF DIFFERENT PARTY AFFILIATIONS MUST RECONCILE AND DOCUMENT ALL UNVOTED, ISSUED, AND SPOILED PAPER BALLOTS AT THE END OF EACH DAY THE POLLING CENTER IS OPEN AND IMMEDIATELY REPORT ANY INVENTORY DISCREPANCIES TO THE COUNTY CLERK.

A. IF UNVOTED PAPER BALLOTS ARE STORED OVERNIGHT AT THE POLLING LOCATION, THE BALLOTS MUST BE SEALED IN CONTAINERS AND STORED IN A LOCKED LOCATION ACCESSIBLE ONLY TO ELECTION OFFICIALS.

Unvoted ballots are offered almost zero security and inventory control once they are mailed out to voters. When unaffiliated voters select only one of two primary ballots to vote, the other ballot is simply unaccounted for and could be returned by an affiliated voter of the wrong party. This is made possible by the failure of Rule 7 to require checking for discrepancy between affiliation and the style of the returned ballot sheet for affiliated primary voters. Therefore these rules are simply ineffective under Colorado's modernized 95+% vote at home central count system. This should be remedied by Rule 7 ensuring a checking of discrepancy between affiliation and style of returned ballot.

New Rule 20.7.2, regarding voting ballots, and subsection (b) is re-codified from current Rule 7.4.8:

1. VOTED BALLOTS

A. ONLY ELECTION OFFICIALS OR CANVASS BOARD MEMBERS SWORN UNDER OATH ARE ALLOWED TO HANDLE VOTED BALLOTS.

Canvass board members are election officials according to CRS.

7.4.8(B) The designated election official must seal and store ballots and return envelopes in a secure ballot area.

A. TRANSPORTATION OF BALLOT BOXES WITH VOTED BALLOTS FROM VSPCs AND BALLOT DROP BOXES TO CENTRAL COUNT FACILITIES:

1. A BIPARTISAN TEAM, OF ELECTION JUDGES AND/OR STAFF, MUST SEAL ALL BALLOT BOXES THAT CONTAIN VOTED BALLOTS SO THAT NO PERSON CAN ACCESS THE BALLOTS WITHOUT BREAKING A SEAL. THE TEAM MUST RECORD ALL SEALS IN THE CHAIN-OF-CUSTODY LOG, VERIFY THAT THE REQUIRED SEALS ARE INTACT, AND SIGN AND DATE THE LOG.

The logs should be retained outside any sealed container so that they may be read upon request without breaking a seal.

1. A BIPARTISAN TEAM, OF ELECTION JUDGES AND/OR STAFF, MUST ACCOMPANY ALL BALLOT BOXES THAT CONTAIN VOTED BALLOTS AT ALL TIMES EXCEPT WHEN THE BALLOT BOX IS LOCATED IN A VAULT OR SECURE PHYSICAL LOCATION.

1. REMEDIES

A. IN THE EVENT THAT A COUNTY DISCOVERS THAT A VIOLATION OF RULE 20.7 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.7.

Once again, the over empowerment of a single person to interpret and execute regulations that lead to sanctions. It is time for Coloradans to consider creation of a state election board that can spread this dangerous power into the hands of persons who have a chance to supervise each other and balance out partisan differences.

New Rule 20.8, concerning security for voting system providers and vendors:

1. SECURITY FOR VOTING SYSTEM PROVIDERS AND VENDORS

1. REMOTE ELECTION PROGRAMMING SERVICES

A. A COUNTY MAY NOT INSTALL OR IMPORT INTO ITS VOTING SYSTEM AN ELECTIO N DATABASE OR PROJECT PROGRAMMED OR CREATED BY THE VOTING SYSTEM PROVIDER USING VOTING SYSTEM COMPONENTS OTHER THAN THOSE OWNED OR LEASED BY THE COUNTY AND SITUATED IN THE COUNTY'S SECURE ELECTIONS FACILITY.

This could eliminate the recent practice of counties to prepare election definitions for neighboring counties who have less resources. This means that all counties must have the capacity to produce these records locally, except for (B) under which a (or is it "the") "voting system provider" is capable of producing it. This Rule does not define "voting system provider". Note that there could be more than one provider of voting system components and there could be service providers for voting systems such as are common in other states.

A. RULE 20.8.1(A) DOES NOT APPLY IF THE VOTING SYSTEM PROVIDER FIRST AFFIRMS ON A FORM PROVIDED BY THE SECRETARY OF STATE THAT:

1. AT ALL TIMES DURING THE ELECTION DATABASE OR PROJECT PROGRAMMING, THE VOTING SYSTEM PROVIDER USED ONLY HARDWARE AND SOFTWARE CERTIFIED FOR USE IN COLORADO, AS CONFIGURED AND VERIFIED DURING TRUSTED BUILD BY THE SECRETARY OF STATE;

1. AT ALL TIMES AFTER INSTALLATION OF TRUSTED BUILD, THE VOTING SYSTEM PROVIDER OPERATED ALL HARDWARE UTILIZED TO PROGRAM THE ELECTION ON A CLOSED NETWORK AND DID NOT CONNECT THE HARDWARE TO THE INTERNET OR ANY INTERNET-CONNECTED DEVICE;

2. AT ALL TIMES DURING THE ELECTION PROGRAMMING PROCESS, THE VOTING SYSTEM PROVIDER COMPLIED WITH THE SECURITY PROTOCOLS FOR REMOVABLE STORAGE DEVICES IN RULE 20.5.3(C); AND

1. THE VOTING SYSTEM PROVIDER PHYSICALLY DELIVERED TO THE COUNTY REMOVABLE STORAGE MEDIA CONTAINING THE FINISHED ELECTION DATABASE OR PROJECT AND DID NOT TRANSMIT USING ANY METHOD CONNECTED OR EXPOSED TO THE INTERNET.

1. VOTING SYSTEM COMPONENT REPLACEMENT OR REPAIR

A. A COUNTY THAT SENDS A VOTING SYSTEM COMPONENT TO A VOTING SYSTEM PROVIDER FOR REPAIR MUST SUBMIT AN INCIDENT REPORT TO THE DEPARTMENT AS REQUIRED BY RULE 11.7.2 AND AN EQUIPMENT ACQUISITION/DISPOSAL FORM TO THE VOTING SYSTEMS TEAM AT THE DEPARTMENT.

A. WHEN THE COUNTY RECEIVES THE REPAIRED COMPONENT, OR RECEIVES A REPLACEMENT COMPONENT, THE COUNTY MUST VERIFY THE SERIAL NUMBER ON THE COMPONENT AND SEAL NUMBERS ON THE SHIPPING CONTAINER MATCH THE NUMBERS

LISTED ON THE TRUSTED BUILD AFFIDAVIT INCLUDED IN THE CONTAINER, OR IF THAT IS NOT POSSIBLE, MUST ARRANGE WITH THE DEPARTMENT TO HAVE TRUSTED BUILD INSTALLED ON THE COMPONENT. THE COUNTY MUST ALSO SUBMIT A COMPLETED ACQUISITION/DISPOSAL FORM TO THE DEPARTMENT AT THE TIME IT RECEIVES THE EQUIPMENT BEFORE IT CAN BE USED IN ANY CAPACITY DURING AN ELECTION.

A. IF EQUIPMENT IS REPAIRED BY A VENDOR ONSITE, THE COUNTY MUST KEEP A MAINTENANCE LOG FOR THE DEVICE THAT MUST CONTAIN THE FOLLOWING:

1. THE MODEL NUMBER, SERIAL NUMBER, AND THE TYPE OF DEVICE;

1. THE SOFTWARE VERSION, AS APPLICABLE;

1. THE PRINTED NAME AND SIGNATURE OF THE VENDOR REPAIRING THE EQUIPMENT; AND

1. THE DATE THE VENDOR WAS ONSITE.

A. A COUNTY MAY NOT ALLOW FOR THE ON-SITE REPAIR OR MAINTENANCE OF A VOTING SYSTEM COMPONENT THAT HAS TRUSTED BUILD SOFTWARE INSTALLED.

This is really getting hard to comprehend or to imagine what the repair logistics look like if the county is unable to repair. We would like to see a more complete explanation.

A. AN EMPLOYEE MUST ESCORT THE VENDOR'S REPRESENTATIVE AT ALL TIMES WHILE ON-SITE. AT NO TIME MAY THE VOTING SYSTEM VENDOR HAVE ACCESS TO ANY COMPONENT OF THE VOTING SYSTEM WITHOUT SUPERVISION BY AN EMPLOYEE.

Please define what kind of employee, if this is a designated employee, or an authorized employee, whom would be issuing the designation or authorization. Please also define the employer.

ON RETURN OF ANY VOTING SYSTEM COMPONENT SENT FOR OFF-SITE MAINTENANCE, THE COUNTY MUST PERFORM AN ACCEPTANCE TEST FOLLOWING THE WRITTEN PROCEDURES PROVIDED BY THE VOTING SYSTEM VENDOR. THE COUNTY MUST MAINTAIN ALL DOCUMENTATION OF THE RESULTS OF THE ACCEPTANCE TESTING ON FILE WITH THE SPECIFIC DEVICE.

1. IF THE MAINTENANCE WAS PERFORMED ON A BMD, THAT BMD MUST BE USED TO GENERATE FIVE BALLOTS FOR USE IN THE ACCEPTANCE TESTING.

1. IF THE MAINTENANCE WAS PERFORMED ON A BALLOT SCANNER, THEN AT LEAST FIVE BALLOTS (A COMBINATION OF BMD-GENERATED BALLOTS AND NON-BMD-

GENERATED BALLOTS—AT LEAST ONE OF EACH) MUST BE TABULATED ON THE SCANNER.

Please address what is the reason this is not at least as strong as the LAT and what is the reason for the low standard of just five ballots.

1. REMEDIES

A. IN THE EVENT THAT A COUNTY OR VOTING SYSTEM PROVIDER DISCOVERS THAT A VIOLATION OF RULE 20.8 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.8.

New Rule 20.9, concerning the security of other election systems. Current Rules 2.16 and 2.17 re-codified to Rule 20.9.1(a) and (b) with amendments:

1. SECURITY OF OTHER ELECTION SYSTEMS

1. Statewide voter registration database (SCORE)

~~2.16~~(A) SCORE username and password administration

~~2.16.1~~(1) The ~~state user administrator~~ SCORE CUSTOMER SUPPORT assigns county user administrator privileges to the individual designated in each county by the county clerk. The county clerk or election administrator must submit a request for county user administrator privilege to ~~state user administrator~~ SCORE CUSTOMER SUPPORT IN WRITING. The request must specifically state the full name of the county employee that is being assigned as a county user administrator.

~~2.16.2~~(2) Each county is limited to two county user administrators. ~~But,~~ BUT a county clerk may apply to the ~~Secretary of State~~ DEPARTMENT for an additional county user administrator.

~~(a)~~(A) The application must be submitted by the county clerk in writing to ~~state user administrator~~ SCORE CUSTOMER SUPPORT and must state the full name of the county employee for which county user administrator privilege is being sought. The application must also state the specific reasons the county clerk is requesting the additional user administrator.

~~(b)~~(B) The ~~state user administrator~~ SCORE CUSTOMER SUPPORT will notify the county clerk in writing whether the request is approved within five business days after receiving the application.

~~2.16.3~~(3) The county user administrator is responsible for security administration and must assign all access privileges, as well as usernames and passwords for county employees and temporary election workers.

~~(a)~~(A) For county employees, the county user administrator must assign a unique username in accordance with the naming conventions provided by the Secretary of State.

~~(b)~~(B) Passwords must be assigned by the county user administrator upon initial authorization and must be changed by users and maintained confidentially.

~~2.16.4~~(4) If a county employee or temporary election worker is no longer employed by the county, the county user administrator must immediately inactivate the username.

~~2.17~~(B) SCORE network security requirements

~~2.17.1~~(1) The county clerk must use only county-controlled access to networks with proper network security controls in place to access SCORE. The county may never use an open or shared public-use network to access SCORE.

~~(a)~~(A) All wireless networks must meet the following minimum requirements:

~~(1)~~(i) WPA2, or above, security must be enabled;

~~(2)~~(ii) Shared wireless passwords or secrets must be changed every three months, at a minimum; and

~~(3)~~(iii) Wireless keys must be a minimum of 14 characters in length and must include at least one number and mixed case letters.

~~(b)~~(B) All networks must employ proper security controls to ensure malicious users cannot connect to the network, intercept SCORE communications, or otherwise attack the SCORE system. These controls must include, at a minimum, network firewalls and securely configured network equipment to prevent common attack mechanisms.

~~2.17.2~~(2) All individuals who access the SCORE system must sign a SCORE Acceptable Use Policy (AUP) before the county provides a SCORE username.

~~(a)~~(A) The county clerk, county SCORE user-administrator, and county elections IT manager, if applicable, must submit their signed AUP to the Secretary of State.

~~(b)~~(B) The county clerk must retain the AUP for each individual who is assigned a SCORE username.

~~(1)~~(i) The Secretary of State will audit the county AUP records for each county selected for annual inspection of its voting

system maintenance records under ~~Rule 20.10.5~~ RULE 20.12.1(A).

(2)(ii) The Secretary of State will suspend access to SCORE for any individual whose AUP is not on file with the county clerk.

~~2.17.3~~(3) If a federal agency notifies a county of a data breach, OR THE COUNTY OTHERWISE KNOWS OF AN ACTUAL OR ~~a targeted~~ POTENTIAL attack on its county network or, SCORE, or OTHER CRITICAL INFRASTRUCTURE IN THE CLERK'S OFFICE, OR A FEDERAL AGENCY provides any other notice concerning an attack or potential attack on critical elections infrastructure, the county must notify the Secretary of State immediately using the contact information provided by the Secretary of State for this purpose. ~~Counties that have physically or logically segmented their elections systems from county networks must only notify the Secretary of State of an elections related data breach or targeted attack.~~

1. BALLOT-ON-DEMAND PRINTERS

A. SOFTWARE ACCESS, SECURITY, AND STORAGE.

- (1) THE COUNTY MUST CHANGE ALL WINDOWS AND BALLOT-ON-DEMAND APPLICATION PASSWORDS AT LEAST ONCE PER CALENDAR YEAR.
- (2) ONLY ELECTION OFFICIALS OR AUTHORIZED VENDOR REPRESENTATIVES MAY OPERATE THE BALLOT-ON-DEMAND SYSTEM.
- (3) THE COUNTY MAY CONNECT THE BALLOT-ON-DEMAND LAPTOP TO AN EXTERNAL NETWORK FOR THE PURPOSE OF CONNECTING TO SCORE ONLY IF THE COUNTY MAINTAINS CURRENT VIRUS PROTECTION, CURRENT OPERATING SYSTEM SECURITY PATCHES, AND IMPLEMENTS FIREWALLS TO PREVENT UNAUTHORIZED ACCESS.
- (4) THE COUNTY MUST STORE THE BALLOT-ON-DEMAND PRINTER, LAPTOP, AND ~~OTHER ELECTED EQUIPMENT~~ PRINTER IS NOT IN USE.

(B) BALLOT RECONCILIATION

1. THE COUNTY MUST RECONCILE BALLOTS PRINTED ON DEMAND IN ACCORDANCE WITH RULES 10.1.1 AND 10.1.2.
1. THE COUNTY MUST MAINTAIN DAMAGED, MISPRINTED, OR UNUSABLE BALLOTS AS ELECTION RECORDS.

1. REMEDIES

A. IN THE EVENT THAT A COUNTY DISCOVERS THAT A VIOLATION OF RULE 20.9 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.9

New Rule 20.10, pertaining to retention and election project backups:

1. RETENTION AND ELECTION PROJECT BACKUPS

1. ELECTION PROJECT BACKUP SECURITY

A. TO ENSURE ELECTION PROJECT BACKUPS HAVE NOT BEEN ALTERED, A COUNTY MUST STORE ANY MEDIA THAT CONTAINS AN ELECTION PROJECT BACKUP IN A SEALED

CONTAINER IN A SECURE EQUIPMENT AREA. THE CONTAINER MUST BE SEALED BY AT LEAST ONE TAMPER-EVIDENT SEAL AND HAVE A CHAIN-OF-CUSTODY LOG.

A. WHEN ACCESSING THE SEALED CONTAINER CONTAINING ANY MEDIA THAT CONTAINS ELECTION PROJECT BACKUPS TWO ELECTION OFFICIALS MUST VERIFY THE SEAL NUMBER(S) AND SIGN AND DATE THE CHAIN-OF-CUSTODY LOG.

A. REMOVEABLE MEDIA USED TO STORE ELECTION PROJECT BACKUPS MUST CONFORM TO THE REMOVEABLE MEDIA SECURITY STANDARDS IN RULE 20.5.4(C). THE MEDIA MAY ONLY BE CONNECTED TO A COMPONENT OF A VOTING SYSTEM WITH AN INTACT TRUSTED BUILD.

A. ANY MEDIA THAT CONTAINS ELECTION PROJECT BACKUPS MAY NOT CONTAIN ANY DATA THAT IS NOT EXPORTED BY THE VOTING SYSTEM.

This one might be a bit too far for practical implementation. Operating system data is bound to be included.

A. ONLY EMPLOYEES OF THE COUNTY CLERK'S OFFICE THAT HAVE PASSED A CRIMINAL BACKGROUND CHECK ACCORDING TO RULE 20.2.1 MAY ACCESS ANY MEDIA THAT CONTAINS AN ELECTION PROJECT BACKUP, EXCEPT ANY INDIVIDUAL WHO IS PROHIBITED FROM HAVING PHYSICAL CONTACT WITH ANY VOTING EQUIPMENT UNDER SECTION 1-5- 607(1), C.R.S. MAY NOT ACCESS ANY MEDIA THAT CONTAINS AN ELECTION PROJECT BACKUP.

Note for any readers learning more about elections: CRS 1-5-607(1) prohibits elected officials of counties of population 100K or more from handling equipment.

1. RETENTION OF VOTING SYSTEM SECURITY RECORDS

A. THE COUNTY MUST MAINTAIN ALL DOCUMENTATION OF SEALS, CHAIN-OF-CUSTODY, TRUSTED BUILD, ACCEPTANCE TESTING, TRANSFER OF EQUIPMENT BETWEEN PARTIES, OR ANY OTHER DOCUMENTS RELATED TO THE PHYSICAL SECURITY OF VOTING SYSTEM COMPONENTS FOR 25 MONTHS AFTER THAT COMPONENT IS NO LONGER IN THE POSSESSION OF A COUNTY.

A. THE COUNTY MUST MAINTAIN THE FOLLOWING AS ELECTION RECORDS UNDER SECTION 1-7-802, C.R.S.:

1. ACCESS LOGS TO SECURE BALLOT AND SECURE EQUIPMENT AREAS;
1. ACCESS LOGS FOR VOTING SYSTEM COMPONENT ACCESS;
1. VIDEO FOOTAGE CREATED UNDER RULE 20.4.2;
1. ELECTION PROJECT BACKUPS REQUIRED TO BE MADE UNDER RULE 11.4.1(A), (B), (D), AND (E);
1. LOGS GENERATED BY THE ELECTION MANAGEMENT SYSTEM SOFTWARE OF THE VOTING SYSTEM IF THOSE LOGS ARE NOT CONTAINED IN THE ELECTION PROJECT BACKUP. THIS DOES NOT INCLUDE LOGS GENERATED OUTSIDE OF THE ELECTION MANAGEMENT SYSTEM SOFTWARE; AND
1. ANY OTHER DOCUMENTS CREATED BY THE COUNTY TO ENSURE THE PHYSICAL SECURITY OF THE VOTING SYSTEM.

A. ALL WRITTEN ENTRIES IN LOGS AND OTHER DOCUMENTATION MUST BE IN PERMANENT INK AND LEGIBLE.

New Rule 20.10.3, including the proposed permanent adoption of New Rule 20.6.3 (re-organized as New Rule 20.10.3) that was temporarily adopted on February 10, 2022:

1. A COUNTY CLERK MAY NOT CREATE OR DISCLOSE, OR PERMIT ANY PERSON TO CREATE OR DISCLOSE, TO ANY PERSON AN IMAGE OF THE HARD DRIVES OF ANY VOTING SYSTEM COMPONENT WITHOUT THE EXPRESS WRITTEN PERMISSION OF THE SECRETARY OF STATE.

If it is so dangerous to create an image of a hard drive, the public deserves to know exactly when and where one was made and who made it. Images of hard drives are regularly made as part of IT backup

processes. We suggest that this Rule should require publication of any instances of written permission by the SOS to make a disk image. Better yet, any decision taken by the SOS pertaining to these new rules ought to be exposed to the public in written form.

1. REMEDIES

A. IN THE EVENT THAT A COUNTY DISCOVERS THAT A VIOLATION OF RULE 20.10 HAS OCCURRED, THEY MUST FILE AN INCIDENT REPORT REQUIRED BY RULE 20.12.2(A).

A. THE DEPARTMENT OF STATE MAY TAKE ANY ACTION UNDER RULE 20.12.2(B) TO REMEDY A VIOLATION OF RULE 20.10.

One of many repeated power grabs to use the overly board term of “any action.”

New Rule 20.11 concerning security of operations:

1. SECURITY OF OPERATIONS

1. CONTINGENCY PLANS

A. THE COUNTY MUST DEVELOP EMERGENCY CONTINGENCY PLANS FOR VOTING EQUIPMENT AND VOTING LOCATIONS IN ACCORDANCE WITH THIS RULE.

A. IN THE EVENT OF A SERIOUS OR CATASTROPHIC EQUIPMENT FAILURE, OR WHEN EQUIPMENT IS REMOVED FROM SERVICE, OR THERE IS NOT ADEQUATE BACKUP EQUIPMENT TO MEET THE REQUIREMENTS OF SECTION 1-5-501, C.R.S., THE COUNTY MUST NOTIFY THE SECRETARY OF STATE THAT THE COUNTY IS USING PROVISIONAL BALLOTS AS AN EMERGENCY VOTING METHOD.

If this is an emergency, how soon is that notification to be made?

A. THE COUNTY CONTINGENCY PLANS AND EVACUATION PROCEDURES MUST ADDRESS EMERGENCY SITUATIONS INCLUDING FIRE, SEVERE WEATHER, BOMB THREAT, CIVIL UNREST, ELECTRICAL BLACKOUT, EQUIPMENT FAILURE, AND ANY OTHER EMERGENCY SITUATIONS THE COUNTY IDENTIFIES.

A. THE COUNTY MUST DEVELOP PROCEDURES TO ADDRESS FAILURES OF SCORE CONTINUITY, WHICH INCLUDES:

1. NETWORK FAILURE,

1. POWER FAILURE THAT LASTS LESS THAN ONE HOUR, AND

1. POWER FAILURE THAT LASTS MORE THAN ONE HOUR.

A. AT LEAST ONE BMD IN EACH VOTER SERVICE AND POLLING CENTER MUST HAVE A BACKUP BATTERY, OR BE CONNECTED TO AN UNINTERRUPTIBLE POWER SUPPLY, SUFFICIENT TO SUSTAIN CONTINUOUS OPERATION FOR A MINIMUM OF TWO HOURS IN THE EVENT OF POWER LOSS.

New Rule 20.11.2 is re-codified from Current Rule 7.16:

~~7.16~~20.11.2 Closure of VSPCs due to emergency condition

~~7.16.1~~(A) If as a result of an extreme weather event, natural disaster, act of God, human made incident, or disruption to, or threat of disruption to critical infrastructure, a county government or other entity closes all day, closes early, or delays the opening of a building where a voter service and polling center is located, then the county clerk may close for the day, close early, or delay the

opening of any voter service and polling center located in those buildings affected.

~~7.16.2~~(B) The county clerk must immediately notify the Secretary of State and the public of any closure or delayed opening of a voter service and polling center under this Rule.

~~7.16.3~~(C) A county clerk must relocate VSPC operations to a backup location in the event a closure would result in the county not meeting their statutory minimum VSPCs. A county clerk must immediately notify the Secretary of State of the backup location that they will relocate to.

~~7.16.4~~(D) The Secretary of State may petition a court under section 1-7-101 (1)(b), C.R.S. to extend the polling hours in a county or statewide if voter service and polling centers are closed or delayed opening under this Rule.

~~7.16.5~~(E) If a county clerk closes or delays the opening of a voter service and polling center under this Rule, then the Secretary of State and county clerk must issue an emergency ballot available under section 1-7.5-115, C.R.S. to any voter who requests it due to the delay or closure.

New Rule 20.12, regarding Secretary of State inspections and remedies and including the proposed permanent adoption of amendments to current Rule 20.10.5 (re-organized as Rule 20.12.1(a)) that was temporarily adopted on February 10, 2022:

1. SECRETARY OF STATE INSPECTIONS AND REMEDIES

1. INSPECTIONS

A. A COUNTY CLERK MUST MAKE AVAILABLE TO THE SECRETARY OF STATE, UPON REQUEST, COUNTY DOCUMENTS AND EQUIPMENT, INCLUDING, BUT NOT LIMITED TO:

1. COUNTY MAINTENANCE RECORDS;

1. CHAIN OF CUSTODY LOGS;

1. TRUSTED BUILD INTEGRITY;

1. WIRELESS STATUS;

1. VIRUS PROTECTION STATUS;

1. PASSWORD STATUS (BIOS, OPERATING SYSTEM, AND APPLICATIONS);

1. ACCESS LOGS;

1. BACKGROUND CHECK DOCUMENTS;

1. SIGNED ACCEPTABLE USE POLICY AGREEMENTS; AND

1. VIDEO SURVEILLANCE.

A. IN ADDITION TO THE DOCUMENTATION LISTED IN RULE 20.12.1(A), THE COUNTY MUST MAKE ALL DOCUMENTATION RELATED TO THE VOTING SYSTEM AND FOR EVERY DEVICE USED IN THE ELECTION AVAILABLE FOR SECRETARY OF STATE INSPECTION.

This rule should require timely notification to the public when such an inspection or SOS record request is made and for what scope of information. It is easy to imagine that such a request could be deemed by a local official to be of the nature of a denial of service attack that deserves better public oversight of the SOS.

New Rule 20.12.2, including the proposed permanent adoption of New Rule 20.15.4 (re-organized within Rule 20.12.2(b)(3)), amended with updated internal cites, that was temporarily adopted on February 10, 2022:

1. REMEDIES

A. INCIDENT REPORT

1. IF A COUNTY DISCOVERS OR DETERMINES THAT A VIOLATION OF ANY PROVISION OF RULE 20 HAS OCCURRED, THEY MUST IMMEDIATELY FILE AN INCIDENT REPORT WITH THE DEPARTMENT OF STATE BEFORE TAKING ANY OTHER ACTION. THE INCIDENT REPORT MUST DESCRIBE IN DETAIL THE INCIDENT AND RULE THAT MAY HAVE BEEN VIOLATED AND ANY OTHER INFORMATION THE DEPARTMENT MAY REQUIRE.

This is unreasonable. Any other action probably would include the local investigation needed to ascertain the contents of the incident report. Does this mean that if a county receives a complaint or report they must pass it on without comment to the SOS? Does this mean that if law enforcement should be engaged, that this law enforcement engagement should be delayed in order to first complete paperwork with the Secretary of State?

1. AFTER AN INCIDENT REPORT IS FILED UNDER THIS RULE, THE DEPARTMENT WILL INVESTIGATE AND DETERMINE WHAT ADDITIONAL ACTION OR INFORMATION, IF ANY, IS REQUIRED.
1. A COUNTY MUST COOPERATE WITH THE INVESTIGATION OF A VIOLATION OF RULE 20. THIS INCLUDES PROVIDING ANY DOCUMENTATION OR ANSWERS REQUESTED BY THE DEPARTMENT DURING THE COURSE OF THE DEPARTMENT'S INVESTIGATION

Overly broad centralization of power in one office without checks and balances.

1. BASED ON THE INFORMATION GATHERED, THE DEPARTMENT MAY TAKE FURTHER ACTION, INCLUDING BUT NOT LIMITED TO, THOSE ACTIONS DESCRIBED IN RULE 20.12.2(B) TO REMEDY THE VIOLATION AND TO ENSURE FUTURE COMPLIANCE WITH RULE 20.

Overly broad centralization of power in one office without checks and balances.

1. A COUNTY'S INTENTIONAL FAILURE TO FILE AN INCIDENT REPORT REQUIRED BY THIS RULE OR FAILURE TO COOPERATE WITH AN INVESTIGATION CONDUCTED BY THE DEPARTMENT OF STATE MAY ALSO RESULT IN ANY OF THE REMEDIES LISTED IN RULE 20.12.2(B).

A. REMEDIES

1. UPON DISCOVERING AND INVESTIGATING A VIOLATION OF RULE 20, THE DEPARTMENT MAY REQUIRE A COUNTY TO TAKE FURTHER ACTION TO REMEDY ANY VIOLATION AND ENSURE FUTURE COMPLIANCE WITH RULE 20.

1. ANY VIOLATION OF RULE 20 MAY RESULT IN THE PROHIBITION OR LIMITATION ON THE USE OF, AS WELL AS DECERTIFICATION OF, A COUNTY'S VOTING SYSTEM OR COMPONENTS IN ACCORDANCE WITH SECTION 1-5-621, C.R.S., AND RULE 21.7.3.

We have seen this language elsewhere in the Rule. It is unclear as to if this implies that there is a security breach or incident that would apply only to the county system where the incident occurred but not in all other counties with the same equipment. For the most part, these really complex and detailed security measures are aimed at protecting everything about the voting system, and almost all of what is being protected is extant in every county that uses the system.

1. IN THE EVENT THAT THE SECRETARY OF STATE DETERMINES THAT AN ELECTION OFFICIAL HAS SHOWN A SERIOUS OR PATTERNED FAILURE TO COMPLY WITH ANY SECURITY REQUIREMENTS FOUND IN STATUTE, THESE RULES, THE CONDITIONS OF USE OF THE VOTING SYSTEM, OR THE ACCEPTABLE USE POLICY AGREEMENT FOR THE VOTING SYSTEM, THE SECRETARY OF STATE MAY TAKE ANY OR ALL OF THE FOLLOWING ACTIONS, INCLUDING BUT NOT LIMITED TO:

A. REQUIRING THE COUNTY CLERK TO SUBMIT A SECURITY REMEDIATION PLAN NO LATER THAN 90 DAYS BEFORE THE NEXT ELECTION

OUTLINING THE PROCEDURES THE COUNTY CLERK WILL FOLLOW TO ENSURE COMPLIANCE WITH THE SECURITY REQUIREMENTS THAT WERE NOT FOLLOWED;

A. PROHIBITING OR LIMITING THE USE OF, AS WELL AS DECERTIFICATION OF, A COUNTY'S VOTING SYSTEM OR COMPONENTS IN ACCORDANCE WITH SECTION 1-5-621, C.R.S., AND RULE 21.7.3;

A. IN ACCORDANCE WITH SECTION 1-1.5-104(2)(A)(II), C.R.S., APPOINTING OBSERVERS AT THE COUNTY EXPENSE TO BE PRESENT WITH THE COUNTY CLERK TO ENSURE COMPLIANCE WITH THE SECURITY REQUIREMENTS; OR

A. REFERRING THE MATTER TO THE ATTORNEY GENERAL OR DISTRICT ATTORNEY FOR POTENTIAL INVESTIGATION AND PROSECUTION UNDER SECTION 1-13-114, C.R.S. OR ANY OTHER APPLICABLE PROVISION.

Amendment to Rule 21.7.3(b), concerning cross-reference change:

a. A county breaks the chain-of-custody for any component of a voting system by allowing any individual not authorized by ~~Rule 20.5.4~~ RULE 20.5.2(B) access to that component;

New Rule 21.11, pertaining to the certification standards for runoff elections and compliance with HB 21-1071:

1. STANDARDS FOR CERTIFYING INSTANT RUNOFF VOTING FUNCTIONALITY

1. RESULTS REPORTING REQUIREMENTS

A. THE VOTING SYSTEM MUST GENERATE A SUMMARY REPORT THAT LISTS THE TOTAL NUMBER OF VOTES FOR EACH CANDIDATE IN EACH ROUND. THE REPORT MUST LIST THE NUMBER OF OVERVOTES, DUPLICATE RANKINGS, SKIPPED RANKINGS, AND BALLOTS WITH FEWER RANKINGS THAN THE MAXIMUM PERMITTED IN THE RACE.

Please change this to per ballot style.

A. THE VOTING SYSTEM MUST GENERATE A BALLOT IMAGE REPORT THAT LISTS THE ORDER IN WHICH THE ELECTOR RANKED THE CANDIDATES FOR EACH BALLOT.

This isn't a "ballot image" under the latest definitions generally agreed to and used by the VVSG. This is instead a CVR. Colorado would do everyone a real favor by sticking with the language that clarifies the record. Ballot images are semi-photographic (but generally low resolution both in luminance -number of bits representing a pixel- and in 2 dimensional spatial coordinates). However, a ballot image should also be produced to back up the CVR and this or 21.11.2 is the place to require it.

A. THE VOTING SYSTEM MUST GENERATE A COMPREHENSIVE REPORT LISTING THE RESULTS IN THE SUMMARY REPORT BY PRECINCT OR BALLOT STYLE AS REQUIRED OR PERMITTED BY SECTION 1-7.5-208(3)(A), C.R.S.

1. DATA EXPORT FORMATS

A. THE VOTING SYSTEM MUST ACCURATELY EXPORT RESULTS DATA BY ROUND SIMULTANEOUSLY FOR ALL ROUNDS FOR USE WITH AN ELECTION NIGHT REPORTING SYSTEM IN .CSV, .JSON, AND .XML FORMATS.

A. THE VOTING SYSTEM MUST ACCURATELY EXPORT A CAST VOTE RECORD IN .CSV, .JSON, AND .XML FORMATS.

This rule should state "a cast vote record and a digital ballot image for every scanned ballot sheet or card." Both of these records should be protected (one per sheet or card) for future authentication by a digital hash or signature that is created under circumstances where the watchers and or the public can see and verify the creation of the authentication code.

1. BALLOT LAYOUT REQUIREMENTS

0. THE VOTING SYSTEM MUST PERMIT THE USER TO LAY OUT BALLOT CARDS CONTAINING BOTH PLURALITY AND INSTANT RUNOFF VOTING CONTESTS ON THE SAME BALLOT CARD OR SEPARATE BALLOT CARDS.

A. THE VOTING SYSTEM MUST PERMIT A USER TO INPUT RANKED VOTING SPECIFIC VOTER INSTRUCTIONS IMMEDIATELY PRECEDING RANKED VOTING CONTESTS.

A. THE VOTING SYSTEM MUST BE ABLE TO SUPPORT RANKING AT LEAST TEN NAMED CANDIDATES AND UP TO TWO WRITE-IN CANDIDATES PER INSTANT RUNOFF CONTEST.

A. THE VOTING SYSTEM MUST ALLOW THE RANKED VOTING CONTESTS TO BE FORMATTED ON PAPER BALLOTS IN THE FOLLOWING WAYS:

1. CANDIDATES LISTED IN COLUMNS AND RANKINGS LISTED IN ROWS.

1. RANKINGS LISTED IN COLUMNS AND CANDIDATES LISTED IN ROWS.

1. TABULATION REQUIREMENTS

A. THE VOTING SYSTEM MUST RECORD ALL VALID VOTER RANKINGS.

A. DURING THE FIRST ROUND OF TABULATION, THE VOTING SYSTEM MUST TABULATE THE FIRST-CHOICE RANKS ON EACH BALLOT.

1. A CANDIDATE WHO RECEIVES OVER 50 PERCENT OF THE FIRST-CHOICE RANKS ON EACH BALLOT IS THE WINNING CANDIDATE, AND THE VOTING SYSTEM MUST STOP TABULATING ANY FURTHER ROUNDS.

This can be misinterpreted. Is the threshold to always be 50 percent. Does the denominator of the 50% calculation only include first choice ranks and not any undervotes? If so, it is subject to a discrepancy caused by missed marks. Ideally the denominator would be the count of voters for whom the cast ballot contained the contest.

1. IF NO CANDIDATE RECEIVES OVER 50 PERCENT OF THE FIRST-CHOICE RANKS ON EACH BALLOT, THE VOTING SYSTEM MUST CONTINUE TO THE NEXT ROUND OF TABULATION.

Whether or not the first round margin is close to 50%, but especially if so, the system should produce the results from the rest of the rounds in order to educate the public about the sense of the electorate (without having to independently access the ballot images or CVRs and calculate themselves.)

A. DURING THE NEXT ROUND OF TABULATION, THE VOTING SYSTEM MUST ENSURE THAT THE CANDIDATE WITH THE FEWEST FIRST-CHOICE RANKS IN THE FIRST ROUND IS ELIMINATED, AND THE ELIMINATED CANDIDATE'S VOTES ARE TRANSFERRED TO EACH BALLOT'S NEXT- RANKED CONTINUING CANDIDATE.

1. IF, AFTER RECEIVING THE TRANSFERRED VOTES, A CONTINUING CANDIDATE RECEIVES OVER 50 PERCENT OF THE VOTES CAST ON ACTIVE BALLOTS, THAT CANDIDATE IS THE WINNING CANDIDATE, AND THE VOTING SYSTEM MUST STOP TABULATING ANY FURTHER ROUNDS.

"Must stop" is contrary to transparency and contrary to the interest of the public in understanding the election. Furthermore, "50 percent of the votes cast on active ballots" means, presumably, that undervotes are not included in the denominator and the 50 percent to determine a win is no longer of the count of voters with ballots containing the contest, but a smaller number, eliminating the effect of those perhaps intentional undervotes that probably reflect lack of interest in supporting the remaining candidates. In other words, the threshold to win is only among voters interested in the candidates remaining viable, thus disenfranchising any other voters.

1. IF NO CANDIDATE HAS OVER 50 PERCENT OF THE VOTES CAST ON ACTIVE BALLOTS AFTER THE SECOND ROUND, THE VOTING SYSTEM MUST REPEAT ADDITIONAL ROUNDS OF TABULATION AS DESCRIBED IN THIS RULE, UNTIL THERE IS A WINNING CANDIDATE.

A. IF THE COMBINED VOTES OF TWO OR MORE CANDIDATES IN THE CURRENT ROUND ARE LESS THAN THE NUMBER OF VOTES FOR THE CONTINUING CANDIDATE WITH THE NEXT-HIGHEST VOTES, THEN THE VOTING SYSTEM MUST ELIMINATE BOTH CANDIDATES SIMULTANEOUSLY.

A. IN ANY ROUND, IF TWO OR MORE CANDIDATES TIE FOR THE LOWEST NUMBER OF VOTES, AND THE VOTING SYSTEM CANNOT ELIMINATE THE CANDIDATES ACCORDING TO THE CRITERION IN SUBSECTION (D), THEN THE VOTING SYSTEM MUST ALLOW THE USER TO

DETERMINE BY LOT WHICH CANDIDATES ARE ELIMINATED IN ACCORDANCE WITH RULE 26.5.5.

A. THE VOTING SYSTEM MUST ALLOW THE USER TO DECIDE WHETHER TO ALLOW SKIPPED RANKINGS OR TO EXHAUST THE BALLOT WHEN A RANKING IS SKIPPED.

User term schedule be defined for all instances of user.

A. THE VOTING SYSTEM MUST ALLOW THE USER TO DECIDE WHETHER TO PAUSE THE TABULATION SESSION AFTER EACH ROUND OR TO CONTINUE UNTIL A WINNER IS DETERMINED OR A MANUAL TIE BREAK FOR ELIMINATION IS REQUIRED.

A. THE VOTING SYSTEM MUST ALLOW THE USER TO DECIDE WHETHER OR NOT TO INCLUDE AS AN OVERVOTE RANKS FOR CANDIDATES FOR WHOM VOTES MAY NOT BE COUNTED, IN ACCORDANCE WITH SECTION 1-4-1001, C.R.S.

A. THE VOTING SYSTEM MUST ALLOW THE USER TO DECIDE WHETHER TO COUNT A RANKING FOR A CANDIDATE FOR WHOM VOTES MAY NOT BE COUNTED, IN ACCORDANCE WITH SECTION 1-4-1001, C.R.S., AS A SKIPPED RANKING OR TO ELEVATE LOWER RANKINGS.

1. BALLOT MARKING DEVICE REQUIREMENTS

A. BALLOT MARKING DEVICES MUST PROHIBIT VOTERS FROM OVERVOTING ANY RANKING.

A. BALLOT MARKING DEVICES MUST PROHIBIT VOTERS FROM SKIPPING RANKINGS.

A. THE VOTING SYSTEM MUST PRESENT CLEAR AUDIO AND VISUAL NOTIFICATIONS IF THE VOTER HAS RANKED FEWER CANDIDATES THAN THE CONTEST'S MAXIMUM PERMITTED NUMBER OF RANKINGS BUT WILL ALLOW THE VOTER TO PROCEED WITH THEIR VOTING SESSION IF THE VOTER CHOOSES TO DO SO.

Please address the following outstanding questions: When is the "contest's maximum permitted number of rankings" different from the number of candidates plus write-ins? Who might decide that?

1. BALLOT ADJUDICATION REQUIREMENTS

A. THE VOTING SYSTEM MUST ALLOW THE USER TO QUEUE BALLOTS WITH THE FOLLOWING CONDITIONS FOR ADJUDICATION BY ELECTION JUDGES:

1. ANY AMBIGUOUS MARK IN ANY RANKING.

1. ANY RANKING THAT RESULTS IN AN OVERVOTE.

1. ANY SKIPPED RANKING.

1. ANY DUPLICATE RANKING.

1. ANY CONTEST IN WHICH A VOTER HAS RANKED FEWER CANDIDATES THAN THE CONTEST'S MAXIMUM PERMITTED NUMBER OF RANKINGS.

[Not shown: current Rule 26.1 is re-codified throughout Rule 1.1. This is shown at the beginning of the document.]

[Not shown: renumbering of current Rules 26.2 through 26.5 to Rules 26.1 through

26.4.] [Not shown: current Rule 26.6 renumbered to Rule 26.5.]

Amendments to current Rule 26.6.3, renumbered to Rule 26.5.3, to ensure proper administration of HB21-1073:

~~26.6.3~~26.5.3 During the ~~second~~ NEXT round of tabulation, the candidate with the fewest first- choice ranks in the first round is eliminated and the eliminated candidate's votes are transferred to each ballot's next-ranked continuing candidate.

Please address the following outstanding questions: Depending upon how skipped ranks are treated? Is the order of candidate elimination determined only by first choice ranks? T

[Not shown: no changes to subsections (a) and (b).]

Amendments to Rule 26.6.4, renumbered to Rule 26.5.4, to ensure the proper administration of HB21-1071 concerning combined votes in the certification system:

~~26.6.4~~26.5.4 In any round, two or more candidates may be eliminated simultaneously if those candidates' combined votes in that round plus the combined votes of all candidates with fewer votes, if any, are less than the number of votes for the candidate with the next highest number of votes. IF THE COMBINED VOTES OF TWO OR MORE CANDIDATES IN THE CURRENT ROUND ARE LESS THAN THE NUMBER OF VOTES FOR THE CONTINUING CANDIDATE WITH THE NEXT- HIGHEST VOTES, THEN THOSE CANDIDATES ARE ELIMINATED.

Amendments to current Rule 26.6.5, renumbered to Rule 26.5.5, concerning cross-reference change:

~~26.6.5~~26.5.5 In any round, if two or more candidates tie for the lowest number of votes, the eliminated candidate must be chosen by lot, unless the candidates may be eliminated simultaneously under ~~Rule 26.6.4~~RULE 26.5.4.

[Not shown: current Rule 26.6.6 renumbered to Rule 26.5.6.]

Amendments to current Rule 26.6.6, renumbered to Rule 26.5.6, concerning cross-reference change:

~~26.6.7~~26.5.6 The designated election official need not report election night results under ~~Rule 41.10.4~~RULE 11.9.4, unless directed by the Secretary of State.

Please address: If not during ENR, when will the results be reported?

[Not shown: current Rule 26.7 renumbered to Rule 26.6.]

Amendments to current Rule 26.7.3, renumbered to Rule 26.6.3, concerning cross-reference change:

~~26.7.3~~26.6.3 During the second round of tabulation, the designated election official must calculate each winning candidate's surplus votes, as described in ~~Rule 26.7.4~~RULE 26.6.4, and transfer those votes proportionately to any continuing candidate.

Amendments to current Rule 26.7.4(c), renumbered to 26.6.4(c), concerning cross-reference change:

a. After calculating a winning candidate's surplus fraction, tabulate the number of votes cast for the next-highest-ranked continuing candidate on every ballot cast for the winning candidate. Then multiply each of those votes cast by the winning candidate's surplus fraction and add the resulting transfer value to any continuing candidate's total as described in ~~Rule 26.7.3(b)~~RULE 26.6.3(B).

It will be difficult to obtain evidence-based confidence out of implementation of this description. Please reconsider.

[Not shown: no changes to subsection (d).]

[Not shown: current Rule 26.7.5 renumbered to Rule 26.6.5.]

Amendments to current Rule 26.7.6, renumbered as Rule 26.6.6, concerning cross-reference change:

~~26.7.6~~26.6.6 The designated election official need not report election night results under ~~Rule 11.10.4~~RULE 11.9.4, unless directed by the Secretary of State.

This looks the same as 26.5.6 and is possibly redundant.

[Not shown: current Rules 26.8 and 26.9 renumbered to Rules 26.7 and 26.8.]

[Not shown: current Rule 26.10 renumbered to Rule 26.9.]

Amendments to current Rule 26.10.4(c), renumbered to 26.9.4(c), concerning cross-reference changes:

(c) For each ranked voting contest, the audit board must hand count the ballots cast, following the counting method set forth in ~~Rule 26.6~~RULE 26.5 for instant-runoff- voting contests, and in ~~Rule 26.7~~RULE 26.6 for single transferable voting contests.