**STATE OF COLORADO**
**Department of State**
1700 Broadway
Suite 200
Denver, CO 80290

**Scott Gessler**
**Secretary of State**

**Suzanne Staiert**
**Deputy Secretary of State**

Please see my comments in marginal boxes like this one.

Thank you.
Mary Eberle

# Help Shape Colorado's Election Rules

Topic: Rules Concerning Voting System Conditions for Use

May 29, 2014

**What is this about?**

Secretary Gessler is considering whether to propose permanent rulemaking to codify Colorado's certified voting equipment conditions for use as administrative rules.

In Colorado, counties may only use voting systems that the Secretary of State has certified as meeting the requirements of state and federal law.[1] The Secretary of State also requires each county to adhere to specific conditions for use of each certified voting system.[2] Currently, there are separate conditions-for-use documents for each of Colorado's four voting-system vendors, even though many of the same conditions apply to all systems. Additionally, already-enacted election rules concerning voting systems have rendered many of the conditions for use superfluous, because these rules restate the requirements found in the conditions.

For these reasons, the Secretary intends to develop a single set of clear and concise administrative rules that ensure each county understands the conditions for using its certified voting system.

The main goals of the proposed rulemaking are to:

- Eliminate redundant requirements that currently appear in each separate conditions-for-use document or in the Secretary of State's Election Rules;
- Clarify that the requirements for using a certified voting system in Colorado are not optional, but rather have the force and effect of law;
- Provide counties with easy-to-follow voting-system requirements in Colorado;
- Create a single source for counties to access voting system conditions for use; and
- Provide an open and transparent process for updating and amending the conditions when necessary.

We invite you to share your thoughts and recommendations as we develop a preliminary draft of the proposed rules. Please review the attached working draft. For your reference, we have also attached copies of the current conditions-for-use documents that include annotations explaining where each condition is or will be addressed—whether in the working draft of proposed rules or in current election rules.

I hope you will use "witness and verify" regarding watchers and not use "observe"-- the watcher rule needs to be strengthened to preserve watcher rights. Watchers need to be at all "stations" or scanners where ballots are being processed, not just one watcher per room or building.

Also, UOCAVA voters need to be warned by clerks that such voters are to return ballots electronically only if there is not a more secure way available to them.

[1] Section 1-5-608.5(3)(a), C.R.S.
[2] Section 1-5-608.5(3)(b), C.R.S.

**Why does the Secretary need my help?**

The Secretary values your feedback and we would very much like to hear your thoughts. We need your help to identify necessary revisions or additional guidance in order to propose a constructive and comprehensive draft rule for consideration during the rulemaking proceedings. Overall, we invite your opinions and recommendations to help shape Colorado's Election Rules.

**How do I submit my comments and what is the deadline?**

You may email your comments to SOS.Rulemaking@sos.state.co.us. To ensure consideration of your comments before we issue the proposed draft, we must receive your comments by 5:00 p.m. on June 6, 2014.

**Will my comments become part of the official record for the anticipated rulemaking?**

Yes, we will incorporate your comments into the official record when we commence with formal rulemaking. Our office will identify your comments as information received in anticipation of rulemaking to support the development of the proposed draft rule. Please note that you will have an additional opportunity to provide testimony and/or written comments regarding the proposed rule during the rulemaking proceeding.

To promote transparency and to help generate discussion, our office will post a copy of your comments on the Secretary of State's website. We appreciate privacy concerns and will redact personal contact information that may appear in your comments prior to posting (including your home address, personal email address, and telephone number). To view the comments that we receive, please visit: http://www.sos.state.co.us/pubs/rule_making/ruleComments.html.

# Working Draft of Proposed Rules

**Office of the Colorado Secretary of State**
**Election Rules**
**8 CCR 1505-1**

**May 29, 2014**

**Disclaimer**:
The following is a working draft concerning Rule 20 (County Security Procedures). The Secretary values your input and is seeking feedback about the proposed revisions before a formal notice of rulemaking.

Please send your feedback by June 6, 2014. Please reference the specific page and line number in your comments. We will consider all comments submitted by this date for inclusion in the official rulemaking draft.

Please note the following formatting key:

| Font effect | Meaning |
|---|---|
| Sentence case | Retained/modified current rule language |
| SMALL CAPS | New language |
| ~~Strikethrough~~ | Deletions |
| *Italic blue font text* | Annotations |

---

*Amendments to Rule 20.1:*

20.1 The county ~~clerk~~ must submit its annual security plan on the form prescribed by the Secretary of State in accordance with section 1-5-616(5), C.R.S.

*Amendments to Rule 20.2.2, regarding general requirements concerning chain-of-custody:*

20.2.2 The county must maintain and document ~~the~~ UNINTERRUPTED chain-of-custody for each voting device FROM THE INSTALLATION OF TRUSTED BUILD TO THE PRESENT, throughout the county's ownership or leasing of the device. FOR VOTING SYSTEMS ACQUIRED BEFORE MAY 28, 2004, THE COUNTY MUST MAINTAIN AND DOCUMENT UNINTERRUPTED CHAIN-OF-CUSTODY FOR EACH VOTING DEVICE FROM THE SUCCESSFUL COMPLETION OF ACCEPTANCE TESTING CONDUCTED ACCORDING TO RULE 20.8.4.

*Amendments to Rule 20.3.1(e), regarding physical locking mechanisms and seals for DREs and ballot marking devices:*

(e) ~~These same procedures also apply to the Judge's Booth Controller (JBC) unit for the Hart InterCivic System.~~ THE COUNTY MUST PROVIDE EACH DRE VOTER A HEADSET WITH AN ADJUSTABLE VOLUME CONTROL.

*Amendments to Rule 20.4.1:*

20.4 Individuals with access to keys, door codes, and vault combinations~~.~~

20.4.1 For employees with access to areas addressed in Rule 20.4.3, the county must state in the security plan each employee's title and the date of the ~~the~~ criminal background check. [Section 24-72-305.6, C.R.S.]

*Amendments to Rule 20.5.2, regarding internal controls for the Voting System:*

20.5.2 In addition to the access controls discussed in Rule 20.4, the county must change all passwords and limit access to the following areas:

(a) Software. The county must change all software passwords once per calendar year prior to the first election. This includes any boot or startup passwords in use, as well as any administrator and user passwords and remote device passwords.

(b) Hardware. The county must change all hardware passwords once per calendar year prior to the first election. This includes any encryption keys, key card tools, supervisor codes, poll worker passwords on smart cards, USB keys, tokens, and voting devices themselves as it applies to the specific system.

(c) ~~Password Management~~ USER PRIVILEGES FOR HARDWARE COMPONENTS. The county must limit access to the ~~administrative passwords to the election management software to two employees. The county must limit access to passwords for all components of the election software and~~ PRIVILEGES AND PASSWORDS FOR hardware COMPONENTS OF THE VOTING SYSTEM to two SUPERVISOR JUDGES AND NO MORE THAN TEN employees. ~~The county may provide an additional ten employees with access to the administrative passwords for the software components, and an additional ten employees with access to the administrative passwords for the hardware components of the voting system.~~

Why add supervisor judges? Seems like more opportunity for partisan mischief.

(D) ADMINISTRATIVE AND USER ACCOUNTS FOR ELECTION MANAGEMENT SYSTEM AND ELECTION DATABASES.

(1) THE COUNTY MAY USE THE ADMINISTRATIVE USER ACCOUNT ONLY TO CREATE INDIVIDUAL USER ACCOUNTS FOR EACH ELECTION DATABASE.

(2) THE COUNTY MUST CREATE INDIVIDUAL USER ACCOUNTS THAT ARE ASSOCIATED AND IDENTIFIED WITH EACH INDIVIDUAL AUTHORIZED USER OF THE ELECTION MANAGEMENT SYSTEM OR ELECTION DATABASE.

Editing note: Use of serial comma (as here) is inconsistent. For best clarity, the serial comma (before the conjunction) should always be used in lists of 3 or more items. See the *Chicago Manual of Style*.

(3) THE COUNTY MUST RESTRICT ACCESS TO EACH INDIVIDUAL USER ACCOUNT WITH A UNIQUE PASSWORD KNOWN ONLY TO EACH INDIVIDUAL USER. AUTHORIZED USERS MUST ACCESS THE ELECTION MANAGEMENT SYSTEM AND ELECTION DATABASE USING HIS OR HER INDIVIDUAL USER ACCOUNT AND UNIQUE PASSWORD.

(4) THE COUNTY MAY GRANT ADMINISTRATIVE PRIVILEGES TO NO MORE THAN TEN INDIVIDUAL USER ACCOUNTS PER ELECTION.

(E) The voting system provider may not have ~~an~~ administrative ~~or application user/operator account, or administrative account access to the accounts.~~ OR USER ACCESS TO THE ELECTION MANAGEMENT SYSTEM OR ELECTION DATABASE. IF A VENDOR PROGRAMS THE ELECTION, THE COUNTY MUST CHANGE THE ADMINISTRATOR, USER, AND DEVICE-LEVEL PASSWORDS BEFORE CONDUCTING THE LOGIC AND ACCURACY TEST.

~~(d)~~ (F) Internet Access. The county ~~must never~~ MAY NOT connect or allow a connection of any voting system component to the Internet. IF THE ELECTION MANAGEMENT SYSTEM WORKSTATION IS EQUIPPED WITH WI-FI CAPABILITY OR A WIRELESS DEVICE, THE COUNTY MUST DISABLE THE WIRELESS CONNECTIVITY.

~~(e)~~ (G) Modem Transmission. The county ~~must never~~ MAY NOT connect any component of the voting system to another device by modem ~~except for the vote tally software~~. THIS PROHIBITION DOES NOT APPLY TO VOTING SYSTEM COMPONENTS THAT MUST COMMUNICATE BY MODEM WITH THE ELECTION MANAGEMENT SYSTEM.

~~(f) Remote voter service and polling centers. At remote voter service and polling centers, the county may use modem functions of optical scanners and DREs only for the purpose of transmitting unofficial results.~~

~~(g)~~ (H) Authorized Employees. The county must include in its security plan ~~each employee's~~ THE title and ~~the~~ date of background checks for ~~employees~~ EACH EMPLOYEE with access to any of the areas or equipment set forth in this Rule. ~~Each~~ THE county must maintain a storage facility access log that details employee name, date, and time of access to the storage facility in which the software, hardware, or components of any voting system are maintained. If access to the storage facility is controlled by use of key card or similar door access system that is capable of producing a printed paper log including the person's name and date and time of entry, such a log must meet the requirements of this Rule. [Section 24-72-305.6, C.R.S.]

*Amendments to Rules 20.8.4 and 20.8.5, regarding equipment maintenance procedures:*

20.8.4 Upon completion of any maintenance, the county must verify or reinstate the trusted build and conduct a full acceptance test of equipment that must, at a minimum,

include the hardware diagnostics test, as indicated in Rule 11, and ~~conduct~~ a mock election in which an employee(s) must cast a minimum of five ballots on the device to ensure tabulation of votes is working correctly. The county must maintain all documentation of the results of the acceptance testing on file with the specific device.

20.8.5 The Secretary of State will annually inspect county maintenance AND CHAIN-OF-CUSTODY records and verify THE INTEGRITY OF trusted build ~~installation~~ on a randomly selected basis.

"and verify THE INTEGRITY OF THE INSTALLED trusted build" would be better.

*Rule 20.9.3(d) formatting correction:*

~~(D)~~ (D) If a seal is broken or chain-of-custody ~~cannot be verified~~ IS UNVERIFIABLE, the county clerk must investigate, document his or her findings, and report the incident to the Secretary of State, as appropriate.

*New Rule 20.11(d), regarding VVPAT security:*

(D) IF THE VVPAT IS EXTERNAL, THE COUNTY MUST SECURE THE CONNECTION BETWEEN THE VVPAT AND THE DRE WITH TAMPER-EVIDENT SEALS, AND MUST MAINTAIN CHAIN-OF-CUSTODY LOGS.

*Amendments to Rule 20.11.2:*

20.11.2 Anonymity. The designated election official must implement measures to protect the anonymity of voters choosing to vote on DREs.

(a) Measures to protect anonymity include:

(1) The county may not keep any record indicating the order in which people voted on the DRE, or which VVPAT record is associated with the voter.

(2) When more than one DRE is available at a voting location, the COUNTY MUST, TO THE EXTENT PRACTICABLE, ALLOW THE voter ~~must be given the choice as to which~~ TO CHOOSE THE DRE ~~they would like~~ HE OR SHE WISHES to vote on~~, to the extent practicable~~.

(b) ~~The county clerk must remove the date/time stamp from any report or export generated from an electronic pollbook. The county clerk may not use this field as a sort method. The county clerk must randomly assign any Record ID, Key ID, or Serial Number stored in the database of votes.~~ THE COUNTY CLERK MAY NOT RELEASE A REPORT GENERATED FROM SCORE THAT INCLUDES A DATE AND TIME STAMP THAT COULD POTENTIALLY IDENTIFY A VOTER WHO CAST A SPECIFIC BALLOT.

I am not a SCORE expert, but this rule reads as though it is all right (because a report exists) if election officials can identify a voter who cast a specific ballot. That violates the spirit of the anonymity of ballots after they are cast.

This rule refers to DREs, but the same problem could result with mail ballots, for which a better approach must be devised and placed in rule. How about requiring that ballot envelopes be shuffled after signature verification and their batches mixed so that the ballots once removed are disconnected from SCORE date and time stamps?

(c) At no time may an election official simultaneously access a VVPAT and the list of voters. ~~Examination of~~ AT LEAST TWO ELECTION JUDGES MUST EXAMINE the VVPAT record ~~must be performed by at least two election officials~~.

(D) THE COUNTY MUST ARRANGE VOTER SERVICE AND POLLING CENTER DREs IN A MANNER THAT PREVENTS ELECTION JUDGES AND OTHER VOTERS FROM OBSERVING HOW A DRE VOTER CASTS HIS OR HER BALLOT.

*Repeal of Rule 20.11.3(c), regarding VVPAT storage:*

~~(c) A master catalog must be maintained for the election containing the complete total number of VVPAT spools used in the election.~~

*New Rule 201.71:*

20.17 VOTING SYSTEM CONDITIONS FOR USE

20.17.1 THE COUNTY MUST USE THE VOTING SYSTEM ONLY ON A CLOSED NETWORK AS DEFINED IN RULE 21.1.6 OR IN A STANDALONE FASHION.

20.17.2 THE COUNTY MUST USE ITS ELECTION MANAGEMENT SYSTEM AS DEFINED IN RULE 21.1.9 OR OTHER EXTERNAL SOLUTION FOR THE ABSTRACT OF VOTES CAST SENT TO THE SECRETARY OF STATE UNDER SECTION 1-10-103(1), C.R.S.

20.17.3 ACCESS LOGS.

(A) IN ADDITION TO THE AUDIT LOGS GENERATED BY THE ELECTION MANAGEMENT SYSTEM, THE COUNTY MUST MAINTAIN ACCESS LOGS THAT RECORD THE FOLLOWING:

(1) THE DATE, TIME, AND USER NAME FOR EACH INSTANCE THAT A USER ENTERS OR EXITS THE SYSTEM OR THE SYSTEM'S REPORT PRINTING FUNCTIONS; AND

(2) MODIFICATIONS TO THE SYSTEM'S HARDWARE, INCLUDING INSERTION OR REMOVAL OF REMOVABLE STORAGE MEDIA, AS DEFINED IN RULE 21.1.15, OR CHANGES TO HARDWARE DRIVERS.

(B) THE COUNTY MAY CREATE AND MAINTAIN THE ACCESS LOGS IN THE MANNER THE COUNTY DEEMS MOST SUITABLE, INCLUDING KEY STROKE RECORDING SOFTWARE, VIDEO SURVEILLANCE RECORDINGS, MANUALLY OR ELECTRONICALLY WRITTEN RECORDS, OR A COMBINATION OF THESE METHODS.

Is video surveillance required by the result of the 2006 court case (Conroy v. Dennis)? I think key stroke recording might be useful. Is there software to make the key strokes easily readable and searchable?



Watching hours of video is a boring job.

20.17.4 THE COUNTY MUST CREATE A BACKUP COPY OF THE ELECTION SETUP RECORDS ON A READ-ONLY, WRITE-ONCE CD, IMMEDIATELY AFTER DOWNLOADING THE FINAL REMOVABLE CARD OR CARTRIDGE.

(A) THE COUNTY MUST IDENTIFY THE MASTER DATABASE NAME AND DATE OF ELECTION ON THE LABEL OF THE BACKUP CD.

(B) THE COUNTY MUST STORE THE BACKUP CD IN A SEALED CONTAINER. TWO ELECTION JUDGES OF DIFFERENT PARTY AFFILIATIONS MUST SIGN AND DATE ENTRIES TO THE CHAIN-OF-CUSTODY LOG FOR THE SEALED CONTAINER.

20.17.5 DREs.

(A) THE COUNTY'S ELECTION JUDGES MUST:

(1) INSTRUCT VOTERS WHO USE THE DRE AUDIO BALLOT FEATURE ON HOW TO PAUSE, REPEAT, AND ADVANCE AUDIO PLAYBACK OF BALLOT INSTRUCTIONS OR TEXT;

(2) TEST THE VVPAT PRINTER IMMEDIATELY AFTER CHANGING THE VVPAT PAPER; AND

(3) LOCK AND RE-SEAL THE VVPAT CANISTER, AND MAKE APPROPRIATE ENTRIES ON THE VVPAT CHAIN-OF-CUSTODY LOG, BEFORE VOTING RESUMES ON THE DRE.

(B) THE COUNTY MUST CONNECT DREs TO UNINTERRUPTIBLE POWER SUPPLIES SUFFICIENT TO SUSTAIN CONTINUOUS OPERATION FOR A MINIMUM OF TWO HOURS IN THE EVENT OF POWER LOSS.

(C) THE COUNTY MUST MAINTAIN LOGS INDICATING ADMINISTRATOR FUNCTION USE.

20.17.6 OPTICAL SCANNERS AS DEFINED IN RULE 21.1.13:

Add something to make clear that this applies to mail ballots as well as polling place ballots. The 2013 sleeves in Boulder County were too small.

(A) WHEN ISSUING BALLOTS, THE COUNTY MUST PROVIDE IN-PERSON VOTERS WITH A SECRECY SLEEVE SUFFICIENT TO CONCEAL A VOTER'S MARKED BALLOT FROM OTHERS IN THE POLLING LOCATION, INCLUDING ELECTION JUDGES.

(B) THE COUNTY MUST RECORD THE OPTICAL SCANNER SERIAL NUMBER ON ALL CHAIN-OF-CUSTODY LOGS AND REPORTS GENERATED BY THE DEVICE.

(C) THE COUNTY MUST CONNECT EACH OPTICAL SCANNER TO UNINTERRUPTIBLE POWER SUPPLIES SUFFICIENT TO SUSTAIN CONTINUOUS OPERATION FOR A MINIMUM OF TWO HOURS IN THE EVENT OF POWER LOSS.

(D) THE COUNTY MUST MAINTAIN LOGS INDICATING ADMINISTRATOR FUNCTION USE.

(E) THE COUNTY MUST PROGRAM EACH OPTICAL SCANNER TO REQUIRE AN OVERRIDE KEY FOR BALLOTS THAT ARE REJECTED BY THE SCANNER.

Bad idea here. The override function allows multiple errors to be affected without human evaluation.

20.18 ES&S VOTING SYSTEM CONDITIONS

20.18.1 IF THE COUNTY MUST PROVIDE LANGUAGE MINORITY ASSISTANCE UNDER SECTION 203 OF THE VOTING RIGHTS ACT (42 U.S.C. §§ 1973 to 1973bb-1), IT MAY NOT USE AN ES&S VOTING SYSTEM.

20.18.2 DREs. THE COUNTY MAY ONLY USE THE NINE INCH SCREEN ON THE VVPAT.

20.18.3 FOR OPTICAL SCANNERS WITH A ZIP DISK DRIVE, THE COUNTY MUST SAVE THE CAST VOTE RECORDS FOR EACH BATCH OF TABULATED BALLOTS TO A ZIP DISK BEFORE SCANNING THE NEXT BATCH.

20.19 HART DRE CONDITIONS. IF A COUNTY SHORTENS A LENGTHY CANDIDATE NAME ON THE VVPAT, IT MUST PROVIDE PRINTED NOTICE OF THE CHANGE TO VOTERS AT THE VOTER SERVICE AND POLLING CENTER.

20.20 SEQUOIA DRE CONDITIONS

20.20.1 THE COUNTY MUST ADD CLARIFYING TEXT TO THE DISPLAY SCREEN DURING THE VVPAT REVIEW PROCESS THAT INSTRUCTS THE VOTER TO REVIEW HIS OR HER BALLOT CHOICES.

20.20.2 THE COUNTY MUST LOCK THE ACTIVATE BUTTON TO PREVENT ITS USE DURING AN ELECTION.

20.20.3 A COUNTY MAY NOT MODIFY THE SCREEN DISPLAY USING AN OVERRIDE.INI FILE WITHOUT APPROVAL FROM THE SECRETARY OF STATE.

I have skipped all the specific conditions for use except those for Hart.

**Conditions for Use – ES&S**

The Testing Board would also recommend the following conditions for use of the voting system. These conditions are required to be in place ***should*** the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, audibility, integrity and availability of the voting system.

**Global Conditions (applies to all components):**

1) Modems and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.

   *This is now addressed by proposed Election Rule 20.5.2(g).*

2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements

   *This is currently addressed by Election Rule 17.2.*

3) Coordination of escrow set-up - Upon certification, voting system manufacturer must coordinate the Escrow of TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 21.11 prior to use in Colorado.

   *This is currently addressed by Election Rule 21.11.*

4) Abstract Report Generation - abstracts used for State reporting must come from Unity Software, or other external solution, rather than from the specific device.

   *This is now addressed by proposed Election Rule 20.17.2.*

5) Trusted Build Verification
   a) The system components do not allow for proper verification of trusted build software. Any breach in custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software components of the system.
   b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of EAC/VSTL and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

   *Global Condition 5(a) is now addressed by proposed Election Rules 20.2.2 and 20.13.1(a). Global Condition 5)(b) is redundant because counties must always utilized certified versions of hardware, software and firmware, without regard to any statements in vendor documentation.*

6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

*This is now addressed by proposed Election Rule 20.1 and 20.5.2(f).*

7) Due to known system failures, the vendor did not submit any information to the Testing Board for testing alternative language requirements. Use of this voting system will be limited to counties that are not required to provide alternative languages to voters under the 2002 Voting Systems Standards referenced by Secretary of State Rule 21.5.2.

*This is now addressed by proposed Election Rule 20.18.1*

**Software Conditions (Unity 3.0.1.1):**

1) System/Database/Network Security Hardening
   a) Because the voting system operates in a non-restricted system configuration containing open file system access to copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.

      *This is now addressed by proposed Election Rules 20.4, 20.5, and 20.7.*

   b) In additional to physical environmental changes, counties shall maintain the integrity of the master Unity databases with one of the following two methods:

      **Option #1 - Create a second (or backup) copy of the Unity database that is created immediately after the point of memory card downloads.** The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the server and proceed with uploading memory cards after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location; or

      *This is now addressed by proposed Election Rule 20.17.4, 20.4, 20.5, and 20.7. The final two sentences are not necessary due to the security protocols applicable to the physical environments and internal controls for election management systems under Election Rules 20.4, 20.5 and 20.7.*

      **Option #2 - Create a second (or backup) copy of the Unity database that is created immediately after the point of downloading all memory cards.** The

copy of the database will be escrowed with the Colorado Secretary of State's office along with the "profile" database. After each of the events described below, the county shall provide both an updated copy of the database to the Secretary of State's office, an updated SQL and Unity audit log, and the forensic analysis of the SQL databases (both profile and election databases) performed by a commercially available forensic tool, identifying changes to database properties since the last report. Events triggering a report update to the Secretary of State include: any download of memory cards, any upload of memory cards, completion of L&A Testing, And COMPLETION of Post-Election Audit. Reports are to be submitted to the Secretary of State's office within 24 hours of the event.

*This option is deleted as unnecessary because proposed Election Rule 20.17.4 requires counties to comply with Option #1 as amended.*

Counties shall indicate in their security plan which option and/or tools they will be executing to meet the security requirements.

*This is unnecessary because all counties using ES&S voting system are required to comply Option #1 above as amended by proposed Election Rule 20.17.4.*

c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the Unity/ERM database. Counties shall prepare for this event with one of two methods:
Option #1 - Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the Unity/ERM software.
When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. During the post-election audit, when the summary report indicated above is created, the difference totals (delta report) are immediately compared to the totals from the report generated by the device at the polling place. If the reports match, the public and the canvass board is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation to the Secretary of State for audit, security and remedy procedures.
During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the Unity/ERM server; OR

Option #2 - Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvas period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the ERM totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

*Software Condition 1(c) is deleted as unnecessary and redundant. The security and audit concerns addressed by this condition are currently covered by Section 1-7-514, C.R.S., and Election Rules 11.3-11.5, and 11.8, and proposed Election Rules 20.2-20.5, 20.7, 20.9, 20.11, and 20.13.*

2) Ballot-On-Demand Restriction.
No provision for ballot reconciliation. This will require counties to have an extra supply of preprinted ballots on hand. Alternatively the county may use the system for ballot on demand printing provided that detailed logs are maintained indicating the number of ballots printed, use and not used by the in-house printing function.

*This is now addressed by proposed Election Rule 20.16.3*

3) Audit Trail Information.
   a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Unity/ERM software for processing by other methods.

   *This is now addressed by proposed Election Rule 20.17.2.*

   b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

Such logs may be achievable by a manner best suitable to each county. Solutions may include the use of key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records or any combination to achieve the necessary audit data. Counties shall report to the Secretary of State's office through their security plans the method of achieving this condition.

*This is now addressed by proposed Election Rule 20.17.3.*

4) Performance Deficiencies.
Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

*This condition has been deleted as unnecessary. Counties that use this system are aware of the potential need for extra time when downloading and uploading memory card devices. Moreover, this condition does not address a security issue.*

5) Provisional Ballots.
The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirement of Rule 10.7.2(g) and users of the system will be required to generate an abstract outside of the voting system.

*The passage of HB 13-1303 and HB 14-1164 has eliminated the need for the condition regarding the processing of federal and state questions only. The abstract and reports provisions of this condition are currently covered by Election Rule 17.*

6) Election Database Creation and Testing.
   a) The system was unable to be fully tested with all Testing Board requirements for ballot layouts as required. Therefore, additional testing will be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This is currently addressed by Election Rules 11.3.2 and 11.3.3.*

   b) Counties are to ensure that ballots are designed and created according to state requirements. The system does not prevent a "backflow" of data changes, nor do system logs accurately represent changes made within the system, and the effect of the changes. Counties using the system shall be required to maintain a log/audit of changes

made to any component of the system after the point when ballots are ordered and/or when any memory cards are created/burned – whichever is earlier.

*This is proposed Election Rule 20.17.3.*

**Precinct Count Scanner Conditions (M100):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

*This is now addressed by proposed Election Rule 20.3.3.*

2) External Power Supply Required.
The device contained internal power to run for 1 ½ HOURS, however under the internal battery included with the system, the device does not count votes correctly. Using an external power source such as a UPS unit providing battery power allows the device to meet the power requirement and count correctly. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component.

*This is now addressed by proposed Election Rule 20.17.6(c).*

3) Device Security Accessibility.
   a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.
   b) County use of voting system will require use of Unity Software to modify the "administrator" password on the voting device.

*This is modified and addressed by proposed Election Rule 20.5.2(b)-(c).*

4) Ballot/Race Conditions Simulation.
Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

5) Audit Trail Information:
   a) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

      *This is now addressed by proposed Election Rule 20.17.6(d).*

   b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Unity software for processing by other methods.

      *This is now addressed by proposed Election Rule 20.17.2.*

   c) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

      *This is now addressed by proposed Election Rule 20.17.6(b).*

   d) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the Unity/ERM software as indicated in Software condition #1c.

      *This is currently addressed by Election Rule 11.3.3*

6) Voting Secrecy.
   Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from ESS) is used for ballots with only one column. For ballots with more than one column, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

   *This is now addressed by proposed Election Rule 20.17.6(a)*

**Central Count Scanner Conditions (M650):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
   Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

   *This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

2) External Battery backup (UPS) Devices Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.

*This is now addressed by proposed Election Rule 20.17.6(c).*

3) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

*This is now addressed by proposed Election Rule 20.17.6(b)*

b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Unity software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2*

c) Batches must be saved to zip disk. Save must take place after each batch.

*This is now addressed by proposed Election Rule 20.18.3*

d) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots counted on the device for the specific races selected in the post election audit:

| Total # of Ballots Counted on Device: | Total # of Ballots to audit: | # of errors requiring escalation: |
|---|---|---|
| 150,000 to 500,000 | 1,250 | 6 |
| 35,001 to 150,000 | 800 | 4 |
| 10,001 to 35,000 | 500 | 3 |
| 3,201 to 10,000 | 315 | 2 |
| 1,201 to 3,200 | 200 | 2 |
| 501 to 1,200 | 125 | 2 |
| 281 to 500 | 80 | 1 |
| 151 to 280 | 50 | 1 |
| 91 to 150 | 32 | 1 |
| 51 to 90 | 20 | 1 |
| 26 to 50 | 13 | 1 |
| 16 to 25 | 8 | 1 |
| 9 to 15 | 5 | 1 |
| 1 to 8 | 3 or 100% if less than 3 | 1 |

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold.

The verification of the hand count of paper ballots shall match the totals generated from the Unity/ERM software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit. If the county or system is not capable of accommodating the requirement of batch size after the outcome of the election is revealed, the highest percentage of ballots shall be used for the audit process.

*This is currently addressed by Election Rule 11.3.3*

4) Ballot/Race Conditions Simulation.

Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be*

*conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of four ballots.*

5) Device Security Accessibility.
Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

*This is modified and addressed by proposed Election Rule 20.5.2(c).*

**DRE Conditions (iVotronic):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
   a) Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

   *This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

   b) Election official shall go into Unity software and change passwords for the iVotronic.

   *This is modified and addressed by proposed Election Rule 20.5.2(b)-(c).*

2) Ballot/Race Conditions Simulation.
Additional County testing shall be required to accommodate ballots with conditions listed. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

3) V-VPAT Paper Record Shall Be Handled per Rule 20.11.3.
Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation.

*This is now addressed by proposed Election Rule 20.6.3 and 20.11.3.*

4) Audit Trail Information:

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Unity software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

b) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

*This is now addressed by proposed Election Rule 20.17.5(c)..*

5) V-VPAT Security.

a) The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

*This is now addressed by proposed Election Rule 20.11.1(d).*

b) Only the 9" screen shall be used when using this system. The vote data can be viewed by the election judges when the paper is changed when the 4.5" screen is used.

*This is now addressed by proposed Election Rule 20.18.2.*

c) The lock on the V-VPAT must be sealed with a tamper evident seal.

*This is now addressed by proposed Election Rule 20.11.1*

d) Only firmware that is loaded during the Trusted Build shall be allowed on the V-VPAT device.

*This is now addressed by proposed Election Rule 20.2.2 and current Election Rule 1.1.30.*

6) Accessible Operation.

a) Due to the inability of the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voter and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

*This is now addressed by proposed Election Rule 20.17.5(a)(1).*

b) A headset with an adjustable volume, which meets the State of Colorado specifications, must be provided.

*This is now addressed by proposed Election Rule 20.3.1(e).*

7) Device Security Accessibility.
   a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

      *This is modified and addressed by proposed Election Rule 20.5.2(c).*

   c) Devices deployed in Colorado shall require the disabling of the PEB activation port due to security concerns discovered through functional testing. A common magnet (example = money clip) can cause a series of attacks and unauthorized control of the device.

      *This is now addressed in proposed Election Rule 20.3.1(b).*

   d) An alternative security measure to 8(b) would be to protect the PEB slot by attaching a lockable cover similar to Figure 8.1 (padlock type); Figure 8.2 (integral keyed lock); or Figure 8.3 (lockable metal PEB well cover).

      *This is now addressed in proposed Election Rule 20.3.1(b).*


Figure 8.1 – Showing PEB slot covered with padlock type enclosure.

Figure 8.2 – Showing PEB slot covered with integral keyed locked enclosure.

Figure 8.3 – Showing PEB slot covered with lockable metal PEB well cover.

(Note: Figures are intended to illustrate concept implementation options, not as requirements of apparatus specification.)

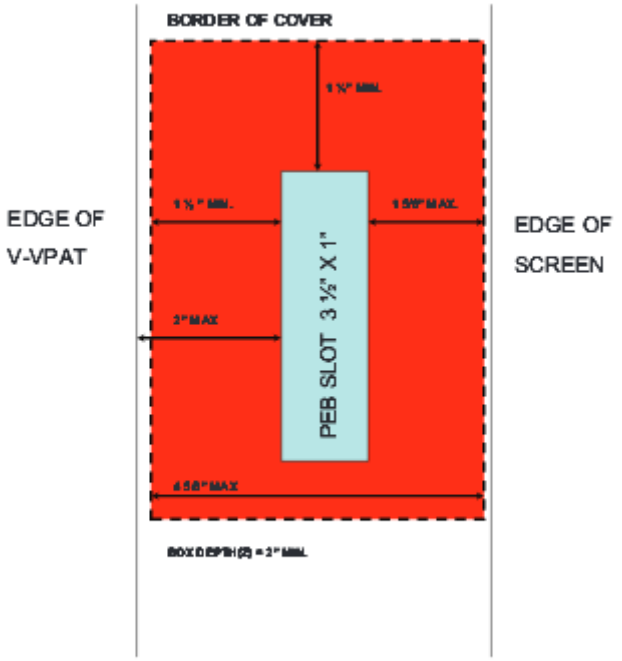


Figure 8.4 – Showing PEB port security cover dimensional requirements.

**Conditions for Use**
**Hart Voting System 6.2.1**
**August 26, 2008**

The Testing Board recommends the following conditions for use of the voting system. The conditions for use shall be implemented by a county.

Any deviation from the conditions provides significant weakness in the security, audibility, integrity and availability of the voting system.

**Global Conditions (applies to all components):**

1) Modems and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.

   *This is now addressed by proposed Election Rule 20.5.2(g).*

2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.

   *This is currently addressed by Election Rule 17.2.*

3) Coordination of escrow set-up - Upon certification, voting system manufacturer must coordinate the Escrow of TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 21.11 prior to use in Colorado.

   *This is currently addressed by Election Rule 21.11.*

4) Abstract Report Generation - abstracts used for State reporting must come from Tally Software, or other external solution, rather than from the specific device.

   *This is now addressed by proposed Election Rule 20.17.2.*

5) Trusted Build Verification
   a) The system components do not allow for proper verification of trusted build software. Any breach in custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software components of the system. Additionally, due to concerns and previous history of software version control with this vendor, counties will be required to audit equipment and submit reports as necessary by the Secretary of State's office to ensure that only the approved components are present on any system in use in this state. Submission of this information shall happen at least once prior to each election and following each election.
   b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of EAC/VSTL and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

In Boulder County, LAT participants have reported forms that were apparently checked off without the person ever looking at the equipment to be checked.

Why not send someone from the SOS office to check the trusted build?

*Global Condition 5(a) is now addressed by proposed Election Rules 20.2.2 and 20.13.1(a). Global Condition 5)(b) is redundant because counties must always utilized certified versions of hardware, software and firmware, without regard to any statements in vendor documentation.*

6) Counties using the voting system shall affirm in their security plan submission that the voting system is used only on a closed network and/or as stand alone devices as required.

*This is now addressed by proposed Election Rule 20.1 and 20.5.2(f).*

7) Use of wireless components is forbidden on the system. Any workstation or laptop that is designed with wireless communications shall have the device disabled and unable to be enabled by anyone other than the system administrator.

*This is now addressed by proposed Election Rule 20.5.2(f).*

8) Election Programming and database distribution shall take place by one of the following three methods:
   a) In the event the county has the software and technical expertise to confidently program their own election, the county shall submit any non-default template to the Secretary of State's office for verification prior to the download of memory cards used in the election. This effort will match the details prescribed under the ballot processing requirements for each device.

   *This is currently addressed by Election Rule 11.4.*

   b) In the event the county has the software but not the expertise to program their own election, counties may choose to coordinate through the manufacturer or other third party company for this service. These companies must be bonded and insured as required under Secretary of State Rule 11. Copies of the database and separated template file must be submitted to the Secretary of State's office as indicated under the ballot processing requirements for each device. In addition, the counties must use the appropriate software to change administrator and device level passwords preventing the manufacturer from knowing such passwords.

   punctua-tion

   *Rule 11 was amended in 2013 to eliminate bonding and insurance requirements for voting system vendors. As such, these requirements are not incorporated into the proposed rules The remaining portions of this condition are addressed by current Election Rule 11.4 and proposed Election Rule 20.5.2(d).*

   why weaken the system? Put bonding and insurance back in, please.

   c) In the event that the county does not have the software to program the election, the county may choose to coordinate through the manufacturer or other third party company for this service. These companies must be bonded and insured as required under Secretary of State Rule 11.
   The county shall follow the following procedures to ensure the integrity of the trusted build and verification of vote totals:

1. Counties shall log any deployment of a vendor to any voting location within the county (this includes pre-election testing, early voting and polling places).
   a. Logs must contain the name of location, vendor name, county person name, date/time, and system serial number at a minimum.
2. Counties shall comply with accompaniment rule (43.8.6.1) for vendors having access to equipment to ensure that a vendor is accompanied at all times by a county employee.
3. Vendor is allowed any access to voting devices as deem necessary by county official.
   a. Counties have the option to quarantine (Secure) the device and request backup equipment from SOS in lieu of vendor accessing voting device.
4. County shall conduct a 100% manual audit of the paper record of all races and ballots cast recorded by the device.
   a. The MBB (Memory card) may be uploaded after audit is verified to match the paper record.
   b. If audit does not match, the device shall be quarantined (secured) and the county shall contact the SOS.
5. For any voting device handled by the voting system vendor, the trusted build shall be reinstalled after the election.
6. Counties shall submit logs and records of hand audits for devices that fall into this category prior to the canvass of official results to the Secretary of State.

*Rule 11 was amended in 2013 to eliminate bonding and insurance requirements for voting system vendors. As such, these requirements are not incorporated into the proposed rules. The remaining provisions of this condition are addressed by existing Election Rules 11.3.2 and 11.3.3 and proposed Election Rules 20.2.2, 20.2.3, and 20.8.3.*

All copies of the database and separated template file must be submitted to the Secretary of State's office as indicated under the ballot processing requirements for each device for the original database and any subsequent changes to the database.
Counties shall identify in the filing of their security plans which method will be executed for a given election.

*This is addressed by current Election Rule 11.4 and proposed Election Rule 20.1.*

**Software Conditions (BOSS and components):**

1) System/Database/Network Security Hardening
   a) Because the voting system operates in a non-restricted system configuration containing open file system access to copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or request a variance from the Secretary of State to create Hart system hardening documentation in lieu of environmental changes. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.

*This is now addressed by proposed Election Rules 20.4, 20.5, and 20.7.*

b) In additional to physical environmental changes, counties shall maintain the integrity of the master Tally databases with one of the following two methods:

**Option #1 - Create a second (or backup) copy of the BOSS, and in some cases the Tally database that is created immediately after the point of memory card downloads.** The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the server/workstation, create a Tally database, if necessary, from the secured copy of the finalized database and proceed with uploading memory cards into Tally after documenting the loading of the backup master database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location;

Be sure to keep this timing. No tallying before election day.

*This is now addressed by proposed Election Rule 20.17.4, 20.4, 20.5, and 20.7. The final two sentences are not necessary due to the security protocols applicable to the physical environments and internal controls for election management systems under Election Rules 20.4, 20.5 and 20.7.*

**OR**

**Option #2 - Create a second (or backup) copy of the BOSS database that is created immediately after the point of downloading all memory cards.** The copy of the database will be escrowed with the Colorado Secretary of State's office along with the template files used. After each of the events described below, the county shall provide both an updated copy of the database to the Secretary of State's office, an updated database audit log, and the forensic analysis of the database performed by a commercially available forensic tool, identifying changes to database properties since the last report. Events triggering a report update to the Secretary of State include: any download of memory cards, any upload of memory cards, completion of L&A Testing, And COMPLETION of Post-Election Audit. Reports are to be submitted to the Secretary of State's office within 24 hours of the event.

*This option is deleted as unnecessary because proposed Election Rule 20.17.4 requires counties to comply with Option #1 as amended.*

Counties shall indicate in their security plan which option they will be executing to meet the security requirements.

*This is unnecessary because all counties using ES&S voting system are required to comply Option #1 above as amended by proposed Election Rule 20.17.4.*

This section is about Hart.

c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased audits for this system. Counties shall verify results with one of two methods:

**Option #1 - Prepare for the upload of memory cartridges as normal.** Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the Tally software. When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. All reports generated shall remain with the memory card for verification purposes.;

**OR**

**Option #2 - Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges).** Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvas period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the software totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

*Software Condition 1(c) is deleted as unnecessary and redundant. The security and audit concerns addressed by this condition are currently covered by Section 1-7-514, C.R.S., and Election Rules 11.3-11.5, and 11.8, and proposed Election Rules 20.2-20.5, 20.7, 20.9, 20.11, and 20.13.*

2) Virus Protection.
The county shall submit for review to the Secretary of State a solution to virus protection that allows for manual updates as required.

*This is now addressed by proposed Election Rules 20.5.2(f), (g) and 20.17.1.*

3) Audit Trail Information.

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally or other software component for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.
Such logs may be achievable by a manner best suitable to each county. Solutions may include the use of key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records or any combination to achieve the necessary audit data. Counties shall report to the Secretary of State's office through their security plans the method of achieving this condition.

*This is now addressed by proposed Election Rule 20.17.3.*

4) Performance Deficiencies.

a) Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

*This condition has been deleted as unnecessary. Counties that use this system are aware of the potential need for extra time when downloading and uploading memory card devices. Moreover, this condition does not address a security issue.*

b) Counties shall ensure that hardware purchased for use of the system matches the specifications of VSTL versions, not the Hart documentation.

*This condition is redundant because counties must always utilized certified versions of hardware, software and firmware, without regard to any statements in vendor documentation.*

Can you figure out a way to make this certification requirement apply to clerks' mail sorting machines like Boulder's B&H?

5) Provisional Ballots.
The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirement

of Rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

*The passage of HB 13-1303 and HB 14-1164 has eliminated the need for the condition regarding the processing of federal and state questions only. The abstract and reports provisions of this condition are currently covered by Election Rule 17.*

6) Election Database Creation and Testing.
   a) The system was unable to be fully tested with all Testing Board requirements for ballot layouts as required. Therefore, additional testing will be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

      *This is currently addressed by Election Rules 11.3.2 and 11.3.3.*

   b) Counties to ensure ballots are designed and created according to state requirements. The vendor may offer a solution that includes non-certified and non-tested proprietary components. Counties may not use any modified template other than what is available as part of the default, and trusted configuration.

      *This is now addressed by proposed Election Rule 20.17.3.*

**Precinct Count Scanner Conditions (eScan):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
   Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

   *This is now addressed by proposed Election Rule 20.3.3.*

2) Ballot Processing.
   a) Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office, have been issued hash values by the Testing Board and have been included with the Trusted Build components of the voting system. Changes to template files must be on file as part of the trusted build in the same manner as the original templates.

      *This is now addressed by proposed Election Rules 20.2.2 and 20.17.3.*

   b) The device shall be set up so that the pollworker is required to use the override key on the back of the device in the event a ballot is rejected. Additionally each ballot or ballot

Why? This seems unhelpful to the voter.

page shall finish being fed through the eScan before the next ballot or ballot page is to be scanned.

*This is not a condition for use because it addresses county business processes rather than system vulnerabilities.*

3) External Power Supply Required.
Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component.

*This is now addressed by proposed Election Rule 20.17.6(c).*

4) Device Security Accessibility.
   a) County use of voting system will be required to modify the "administrator" password on the voting devices preventing the manufacturer access to the device by means of a password. Refer to Global Condition #8 for additional details on this condition and optional procedures to mitigate security concerns by this deficiency.

   *This is modified and addressed by proposed Election Rule 20.5.2.*

   b) County shall coordinate with the vendor and submit to the state the plan for an approved transfer container for securing ballots after the close of polls on the device.

   *This is now addressed by proposed Election Rule 20.9.*

   c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the Tally software as indicated in Software condition #1c.

   *This is currently addressed by Election Rule 11.3.3*

5) Audit Trail Information:
   a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally software for processing by other methods.

   *This is now addressed by proposed Election Rule 20.17.2.*

   b) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

   *This is now addressed by proposed Election Rule 20.17.6(b).*

c) Due to errors in processing and auditing information processed by the device, the device will be limited in functionality to only using serial numbered ballots.

*This provision has been deleted as contrary to section 1-5-407(7), C.R.S.*

d) Election official shall not reset the device without first creating an event and backing up the device in order to maintain a complete history of the audit logs.

*This condition was developed from the perceived failure of the eScan to the meet the requirements of Section 1-5-615(1)(p). But the SERVO can produce the audit log required by this statute. As such, this condition has been deleted as unnecessary.*

6) Voting Secrecy.
Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from Hart) is used for ballots up to 14" in length or shorter. For ballots outside of this description, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

*This is now addressed by proposed Election Rule 20.17.6(a).*

**Central Count Scanner Conditions (Ballot Now/Scanners):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule20.3, 20.8, and 20.9.2(a)(3).*

2) Ballot Processing.
a) Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office, have been issued hash values by the Testing Board. Changes to template files must be on file as part of the trusted build in the same manner as the original templates.

*This is addressed by proposed Election Rule 20.2.2.*

b) Counties shall manually resolve all races containing an overvote or a vote for a write-in candidate and shall be required to use AutoResolve for all undervotes when resolving ballot images.

*This is currently addresses by Election Rule 18.*

3) External Power Supply Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.

*This is now addressed by proposed Election Rule 20.17.6(c).*

4) Audit Trail Information:

a) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

*This is now addressed by proposed Election Rule 20.17.6(b)*

b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the appropriate software module for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2*

c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots counted on the device for the specific races selected in the post election audit:

| Total # of Ballots Counted on Device: | Total # of Ballots to audit: | # of errors requiring escalation: |
|---|---|---|
| 150,000 to 500,000 | 1,250 | 6 |
| 35,001 to 150,000 | 800 | 4 |
| 10,001 to 35,000 | 500 | 3 |
| 3,201 to 10,000 | 315 | 2 |
| 1,201 to 3,200 | 200 | 2 |
| 501 to 1,200 | 125 | 2 |
| 281 to 500 | 80 | 1 |
| 151 to 280 | 50 | 1 |
| 91 to 150 | 32 | 1 |
| 51 to 90 | 20 | 1 |
| 26 to 50 | 13 | 1 |
| 16 to 25 | 8 | 1 |
| 9 to 15 | 5 | 1 |
| 1 to 8 | 3 or 100% if less than 3 | 1 |

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate

identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold.
The verification of the hand count of paper ballots shall match the totals generated from the Tally software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

*This is currently addressed by Election Rule 11.3.3*

5) Network Access/Availability.
The voting system must be used with no network connectivity between devices/units and software. Only a direct connection (SCSI, IEE 1394(i.e. Firewire), etc.) between scanner and workstation will be allowed.

*This is now addressed by proposed Election Rule 20.5.2(f).*

**DRE Conditions (eSlate):**

1) External Power Supply Required.
Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component to accommodate a 120 minute short coming experienced by the Testing Board during testing of the device.

*This is now addressed by proposed Election Rule 20.17.6(c).*

2) Intrusion Seals for Protection of Trusted Build Firmware.
   a) Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rules 20.3, 20.8, and 20.9.2(a)(3).*

   b) Election official shall be required to change passwords on the JBC preventing the manufacturer to have access by means of password to the device. Refer to Global Condition #8 for additional details on this condition and optional procedures to mitigate security concerns by this deficiency.

*This is now addressed by proposed Election Rules 20.5.2(c), (e).*

3) Ballot Processing.

Counties shall ensure that all election programming and layout features have been designed with template files that have been submitted to the Secretary of State's office, have been issued hash values by the Testing Board and have been included with the Trusted Build components of the voting system. Changes to template files must be on file as part of the trusted build in the same manner.

*This is now addressed by proposed Election Rules 20.2.2 and 20.17.3.*

4) V-VPAT Paper Record Shall Be Handled per Rule 11.6.
   a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.

Add "transportation and"

*This is now addressed by proposed Election Rule 20.6.3 and 20.11.3.*

   b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

*This is now addressed by proposed Election Rule 20.17.5(a)(2).*

5) Audit Trail Information:
   a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the Tally software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

   b) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

*This is now addressed by proposed Election Rule 20.17.6(d).*

   c) Election official shall not reset the device without first creating an event and backing up the device in order to maintain a complete history of the audit logs.

*This condition was developed from the perceived failure of the eScan to the meet the requirements of Section 1-5-615(1)(p). But the SERVO can produce the audit log required by this statute. As such, this condition has been deleted as unnecessary.*

6) V-VPAT Security.
   a) The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

*This is now addressed by proposed Election Rule 20.11.1(d).*

b) The lock on the V-VPAT unit must be sealed with a tamper-evident seal.

*This is now addressed by proposed Election Rule 20.11.1*

7) Accessible Operation.

a) Due to the inability of the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voter and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

*This is now addressed by proposed Election Rule 20.17.5(a)(1).*

b) A headset with an adjustable volume, which meets the State of Colorado specifications, must be provided.

*This is now addressed by proposed Election Rule 20.3.1(e)*

8) V-VPAT Truncation.

Due to space limitations on the paper tape, the V-VPAT may truncate lengthy candidate names. In order to mitigate this issue, during the conduct of Logic and Accuracy Testing counties shall determine whether or not truncation will occur. If there is any indication of truncation, printed notice will be provided to the voters prior to voting on the DRE.

*This is now addressed by proposed Election Rule 20.19.*

**Conditions for Use – PREMIER**

The Testing Board would also recommend the following conditions for use of the voting system. These conditions are required to be in place ***should*** the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, audibility, integrity and availability of the voting system.

**Global Conditions (applies to all components):**

1) Modems and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.

   *This is now addressed by proposed Election Rule 20.5.2(g).*

2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.

   *This is currently addressed by Election Rule 17.2.*

3) Coordination of escrow set-up - Upon certification, voting system manufacturer must coordinate the Escrow of TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.

   *This is currently addressed by Election Rule 21.11.*

4) Abstract Report Generation - abstracts used for State reporting must come from GEMS Software, or other external solution, rather than from the specific device.

   *This is now addressed by proposed Election Rule 20.17.2.*

5) Trusted Build Verification (all software and firmware components)
   Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of EAC/VSTL and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

   *This condition redundant because counties must always utilized certified versions of hardware, software and firmware, without regard to any statements in vendor documentation.*

6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

   *This is now addressed by proposed Election Rule 20.1 and 20.5.2(f).*

**Software Conditions (GEMS 1-18-24):**

1) System/Database/Network Security Hardening
   a) Because the voting system operates in a non-restricted system configuration containing open file system access to copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.

      *This is now addressed by proposed Election Rules 20.4, 20.5, and 20.7.*

   b) In additional to physical environmental changes, counties shall create a second (or backup) copy of the GEMS database that is created immediately after the point of memory card downloads. The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location.

      *This is now addressed by proposed Election Rule 20.17.4, 20.4, 20.5, and 20.7. The final two sentences are not necessary due to the security protocols applicable to the physical environments and internal controls for election management systems under Election Rules 20.4, 20.5 and 20.7.*

   c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the GEMs database. Counties shall prepare for this event with one of two methods:

      Option #1 - Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the GEMS software.

      When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. During the post-election audit, when the summary report indicated above is created, the difference totals (delta report) are immediately compared to the totals from the report generated by the device at the polling place. If the reports match, the public is ensured that the totals from the

polling place match the totals from the county server. If the totals are different, the county is to report the situation to the Secretary of State for audit, security and remedy procedures.
During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; OR
Option #2 - Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvas period, with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the GEMS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

*Software Condition 1(c) is deleted as unnecessary and redundant. The security and audit concerns addressed by this condition are currently covered by Section 1-7-514, C.R.S., and Election Rules 11.3-11.5, and 11.8, and proposed Election Rules 20.2-20.5, 20.7, 20.9, 20.11, and 20.13.*

2) Ballot-On-Demand Restriction.
No provision for ballot reconciliation. This will require counties to have an extra supply of preprinted ballots on hand. Alternatively the county may use the system for ballot on demand printing provided that detailed logs are maintained indicating the number of ballots printed, use and not used by the in-house printing function.

*This is now addressed by proposed Election Rule 20.16.3*

3) Audit Trail Information.
   a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the GEMS software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.
Such logs may be achievable by a manner best suitable to each county. Solutions may include the use of key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records or any combination to achieve the necessary audit data. Counties shall report to the Secretary of State's office through their security plans the method of achieving this condition.

*This is now addressed by proposed Election Rule 20.17.3.*

4) Performance Deficiencies.
Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

*This condition has been deleted as unnecessary. Counties that use this system are aware of the potential need for extra time when downloading and uploading memory card devices. Moreover, this condition does not address a security issue.*

5) Provisional Ballots.
The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirement of Rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

*The passage of HB 13-1303 and HB 14-1164 has eliminated the need for the condition regarding the processing of federal and state questions only. The abstract and reports provisions of this condition are currently covered by Election Rule 17.*

**Precinct Count Scanner Conditions (1.96.6):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

*This is currently addressed by Election Rule 20.3.3.*

2) Device Security Accessibility.
   a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.
   b) Due to exposure of passwords, the vendor and the county shall ensure that operators are adequately trained to protect the visibility of the password during use.

   *This is modified and addressed by proposed Election Rule 20.5.2(b)-(c).*

3) Ballot/Race Conditions Simulation.
   Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

   *This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

4) Audit Trail Information:
   a) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

      *This is now addressed by proposed Election Rule 20.17.6(b).*

   b) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

      *This is now addressed by proposed Election Rule 20.17.6(d).*

   c) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the GEMS software for processing by other methods.

      *This is now addressed by proposed Election Rule 20.17.2.*

   d) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the

verification of the hand count of paper ballots to match the totals generated from the GEMS software as indicated in Software condition #1c.

*This is currently addressed by Election Rule 11.3.3*

**Central Count Scanner Conditions (2.0.12):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State.

*This is addressed by proposed Election Rule20.3, 20.8, and 20.9.2(a)(3).*

2) Ballot Processing.
   a) Counties will be required to pre-process all folded ballots that are counted by the voting device. Specifically, operators will presort ballots to detect for appearances of holes punched in the ballot. Ballots with holes in them shall be duplicated onto new ballots by a duplication board as required. Operators of the system shall be adequately trained in the processing and understanding of error messages produced by the device which sometimes represent the correct problem and many times do not.

   *This is addressed by current Election Rule 18.3*

   b) In the event of a recount, the county will have the voting system technician on-site to recalibrate the scanning devices to the sensitivity settings required for testing the device as required by Secretary of State Rule 27.4.2(d). Alternatively, the counties shall perform necessary testing to document and demonstrate that the auto-calibration feature of the device is functioning prior to the counting of ballots for the recount.

   *This is addressed by current Election Rule 18.3.2(f)(1)*

3) External Power Supply Required.
Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.

*This is now addressed by proposed Election Rule 20.17.6(c).*

4) Audit Trail Information:
   a) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

   *This is now addressed by proposed Election Rule 20.17.6(b).*

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots counted on the device for the specific races selected in the post election audit:

| Total # of Ballots Counted on Device: | Total # of Ballots to audit: | # of errors requiring escalation: |
|---|---|---|
| 150,000 to 500,000 | 1,250 | 6 |
| 35,001 to 150,000 | 800 | 4 |
| 10,001 to 35,000 | 500 | 3 |
| 3,201 to 10,000 | 315 | 2 |
| 1,201 to 3,200 | 200 | 2 |
| 501 to 1,200 | 125 | 2 |
| 281 to 500 | 80 | 1 |
| 151 to 280 | 50 | 1 |
| 91 to 150 | 32 | 1 |
| 51 to 90 | 20 | 1 |
| 26 to 50 | 13 | 1 |
| 16 to 25 | 8 | 1 |
| 9 to 15 | 5 | 1 |
| 1 to 8 | 3 or 100% if less than 3 | 1 |

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold.

The verification of the hand count of paper ballots shall match the totals generated from the GEMS software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

*This is currently addressed by Election Rule 11.3.3*

5) Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

6) Network Access/Availability.
The voting system must be used with no network connectivity between devices/units and software. Only a closed LAN connection may be used with necessary hardware for port replication and local IP address assignments as tested.

*This is addressed by proposed Election Rule 20.5.2(f).*

**DRE Conditions (TSx 4.6.4 – C and D models):**

1) V-VPAT Paper Record Shall Be Handled per Rule 11.6.
   a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.

      *This is now addressed by proposed Election Rule 20.6.3 and 20.11.3.*

   b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

      *This is now addressed by proposed Election Rule 20.17.5(a)(2).*

2) Accessible Distances.
Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer's stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4" in length. Should the counties use the DRE in the stand with a reach stick, the counties shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

*This is currently addressed by section 1-5-704, C.R.S.*

3) Accessible Operation.
Due to the inability of the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voter and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

*This is now addressed by proposed Election Rule 20.17.5(a)(1).*

4) Additional Privacy Screen Required.
Required privacy conditions can not be met with attached device privacy panels without also installing accessory screen made by manufacturer; alternatively this condition could be achieved with the use of a computer monitor polarized privacy screen. Counties shall deploy touch screen units in such a manner that voters and judges cannot easily walk behind other voters while processing their vote.

*This is addressed by proposed Election Rule 20.11.2.*

**VC Programmer Conditions:**
Version 4.6.1 - NONE
**Voter Card Encoder Conditions:**
Version 1.3.2 - NONE
**Key Card Tool Conditions:**
Version 4.6.1 - NONE

**Conditions for Use – SEQUOIA**

The Testing Board would also recommend the following conditions for use of the voting system. These conditions are required to be in place ***should*** the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, audibility, integrity and availability of the voting system.

**Global Conditions (applies to all components):**

1) Modems and other telecommunication devices may not be used on any subsystem component - system provider was unable to meet or provide prerequisite FIPS 140/180 certifications.

   *This is now addressed by proposed Election Rule 20.5.2(g).*

2) Provisional ballots must be processed separately from non-conditional ballots - system subcomponents are unable to functionally differentiate and correctly process to Colorado specific requirements.

   *This is currently addressed by Election Rule 17.2.*

3) Coordination of escrow set-up - Upon certification, voting system manufacturer must coordinate the Escrow of TRUSTED BUILD software with SOS escrow, or third party escrow service as required by Rule 11 prior to use in Colorado.

   *This is currently addressed by Election Rule 21.11.*

4) Abstract Report Generation - abstracts used for State reporting must come from WinEDS Software, or other external solution, rather than from the specific device.

   *This is now addressed by proposed Election Rule 20.17.2.*

5) Trusted Build Verification (all software and firmware components)
   a) The system components do not allow for proper verification of trusted build software. Any breach in custody and/or other security incidents will require the rebuild of the component with the state trusted build software. This requirement applies to all voting devices, firmware and software components of the system.
   b) Counties shall ensure that hardware, software and firmware purchased for use of the system matches the specifications of EAC/VSTL and/or State Certified and trusted versions, not to the version presented in the vendor documentation.

   *Global Condition 5(a) is now addressed by proposed Election Rules 20.2.2 and 20.13.1(a). Global Condition 5)(b) is redundant because counties must always utilized certified versions of hardware, software and firmware, without regard to any statements in vendor documentation.*

6) Counties using the voting system shall testify through their security plan submission that the voting system is used only on a closed network.

*This is now addressed by proposed Election Rule 20.1 and 20.5.2(f).*

**Software Conditions (WinEDS 3.1.074):**

1) System/Database/Network Security Hardening
   a) Because the voting system operates in a non-restricted system configuration containing open file system access to copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. Counties shall submit their plan for approval to the Secretary of State's office to be included in the County Security Plan on overcoming these conditions through county environmental and/or procedural changes where possible.

      *This is now addressed by proposed Election Rules 20.4, 20.5, and 20.7.*

   b) In additional to physical environmental changes, counties shall maintain the integrity of the master WinEDS databases with one of the following two methods:

      **Option #1 - Create a second (or backup) copy of the WinEDS database that is created immediately after the point of memory card downloads.** The backup copy shall be stored on closed CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals stored in a sealed or lockable transfer case that is stored in a limited access area. On election day, the designated election official shall load the sealed copy of the database onto the system. After loading the sealed database copy, the county shall re-secure the database with seals (updating necessary logs) in the limited access location; or

      *This is now addressed by proposed Election Rule 20.17.4,. The final two sentences are not necessary due to the security protocols applicable to the physical environments and internal controls for election management systems under Election Rules 20.4, 20.5 and 20.7.*

      **Option #2 - Create a second (or backup) copy of the WinEDS database that is created immediately after the point of downloading all memory cards.** The copy of the database will be escrowed with the Colorado Secretary of State's office along with the "profile" database. After each of the events described below, the county shall provide both an updated copy of the database to the Secretary of State's office, an updated SQL and WinEDS audit log, and the forensic analysis of the SQL databases (both profile and election databases) performed by a commercially available forensic tool, identifying changes to database properties since the last report. Events triggering a report update to the Secretary of State

include: any download of memory cards, any upload of memory cards, completion of L&A Testing, And COMPLETION of Post-Election Audit. Reports are to be submitted to the Secretary of State's office within 24 hours of the event.

*This option is deleted as unnecessary because proposed Election Rule 20.17.4 requires counties to comply with Option #1 as amended.*

Counties shall indicate in their security plan which option they will be executing to meet the security requirements.

*This is unnecessary because all counties using ES&S voting system are required to comply Option #1 above as amended by proposed Election Rule 20.17.4.*

c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post-election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the WinEDS database. Counties shall prepare for this event with one of two methods:

Option #1 - Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the WinEDS software.

When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. During the post-election audit, when the summary report indicated above is created, the difference totals (delta report) are immediately compared to the totals from the report generated by the device at the polling place. If the reports match, the public is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation to the Secretary of State for audit, security and remedy procedures.

During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; OR

Option #2 - Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process can take place any time after the close of polls including through the canvas period, with

observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the WinEDS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

*Software Condition 1(c) is deleted as unnecessary and redundant. The security and audit concerns addressed by this condition are currently covered by Section 1-7-514, C.R.S., and Election Rules 11.3-11.5, and 11.8, and proposed Election Rules 20.2-20.5, 20.7, 20.9, 20.11, and 20.13.*

2) Audit Trail Information.

a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

b) Operators of the system shall also be required to maintain logs indicating use of the report printing functions of the software, and detailed information to changes of the system including hardware changes which shall include: insert removable media, remove removable media, modify system hardware drivers, modify system physical hardware, and any other system property changes made by either judges or other trusted staff. Logs shall be maintained physically in a file outside or separate from the database, which is NOT accessible for review and/or modification by user/operator accounts on the system, but that is readily accessible to election officials or other interested party.

*This is now addressed by proposed Election Rule 20.17.3.*

3) Trusted Build Protection.

Applies to WinEDS software and custom components of SQL server as applicable. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is now addressed by proposed Election Rules 20.2.2 and 20.13.1(a).*

4) Performance Deficiencies.

Due to failures in performance, counties shall allow extra time for downloads and uploads of memory card devices. This may impact programming, testing and use of the system on election night. Counties shall ensure trusted staff is properly trained on this issue and accommodating the allowable time required for programming memory devices.

*This condition has been deleted as unnecessary. Counties that use this system are aware of the potential need for extra time when downloading and uploading memory card devices. Moreover, this condition does not address a security issue.*

5) Provisional Ballots.
The software is not capable of processing provisional ballots internally to accept federal and state only questions. A procedure outside of the voting system will be required. Additionally, the abstracts and reports created by the software do not meet the requirement of Rule 41.6.3(g) and users of the system will be required to generate an abstract outside of the voting system.

*The passage of HB 13-1303 and HB 14-1164 has eliminated the need for the condition regarding the processing of federal and state questions only. The abstract and reports provisions of this condition are currently covered by Election Rule 17.*

6) Election Database Creation and Testing.
The system relies heavily on an external program called BPS which typically is used for importing the ballot setup process into WinEDS. Since this program is to be considered non-trusted and is not third party as it is made by the voting system manufacturer, the program shall only be able to receive data from WinEDS. WinEDS shall not be used to import data from BPS, unless the data is in a static import file format such as flat file, csv, txt, or similar which can be imported without the use of vendor proprietary software. Additional testing will therefore be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 4 ballots of each style that contain the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This is currently addressed by Election Rules 11.3.2 and 11.3.3.*

**Precinct Count Scanner Conditions (Insight/Insight Plus):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is now addressed by proposed Election Rule 20.3.3.*

2) External Power Supply Required.
The device contained internal power to run for three hours, however under the internal battery included with the system, the device did not count votes correctly. Using an external power source such as a UPS unit providing battery power allows the device to meet the power requirement and count correctly. Counties shall purchase and use an

external power supply that meets or exceeds the vendor's recommendation for the component.

*This is now addressed by proposed Election Rule 20.17.6(c).*

3) Device Security Accessibility.
   a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.
   b) County use of voting system will require use of WinEDS Software to modify the "administrator" password on the voting device.

*This is modified and addressed by proposed Election Rule 20.5.2(b)-(c).*

4) Ballot/Race Conditions Simulation.
Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

5) Audit Trail Information:
   a) Operators of the system shall also be required to maintain logs indicating use of the administrator functions of the device by either judges or other trusted staff.

      *This is now addressed by proposed Election Rule 20.17.6(d).*

   b) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

      *This is now addressed by proposed Election Rule 20.17.2.*

   c) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper ballots to match the totals generated from the WinEDS software as indicated in Software condition #1c.

*This is currently addressed by Election Rule 11.3.3*

6) Voting Secrecy.
Insufficient privacy of ballot was detected using secrecy sleeve. Election administrators must ensure system secrecy sleeve (from Sequoia) is used for ballots up to 14". For longer ballots, the counties shall create a secrecy sleeve to accommodate the deficiency and submit design form to Secretary of State for approval.

*This is now addressed by proposed Election Rule 20.17.6(a)*

**Central Count Scanner Conditions (400 C):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

2) System/Database/Network Security Hardening
Because the voting system operates in a non-restricted system configuration containing open file system access to copy, open and overwrite without detection, election vote content database files outside of election management system application by third-party tools, counties will be required to modify their physical environmental conditions, or work with current Sequoia documentation (not currently tested) and request variance from the Secretary of State to use Sequoia hardening documentation in lieu of environmental changes. If approved, counties shall submit their plan for approval to the Secretary of State's office on overcoming these conditions through one of the two stated processes.

*This is now addressed by proposed Election Rules 20.4, 20.5, and 20.7.*

3) External Power Supply Required.
Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component. Acceptable power supply sources include generators and other facility based solutions.

*This is now addressed by proposed Election Rule 20.17.6(c).*

4) Audit Trail Information:
   a) Judges shall be required to include device serial number on all reports regarding the use of the device. Additionally, the county shall include the device serial number on applicable reports from the device.

*This is now addressed by proposed Election Rule 20.17.6(b)*

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots counted on the device for the specific races selected in the post election audit:

| Total # of Ballots Counted on Device: | Total # of Ballots to audit: | # of errors requiring escalation: |
|---|---|---|
| 150,000 to 500,000 | 1,250 | 6 |
| 35,001 to 150,000 | 800 | 4 |
| 10,001 to 35,000 | 500 | 3 |
| 3,201 to 10,000 | 315 | 2 |
| 1,201 to 3,200 | 200 | 2 |
| 501 to 1,200 | 125 | 2 |
| 281 to 500 | 80 | 1 |
| 151 to 280 | 50 | 1 |
| 91 to 150 | 32 | 1 |
| 51 to 90 | 20 | 1 |
| 26 to 50 | 13 | 1 |
| 16 to 25 | 8 | 1 |
| 9 to 15 | 5 | 1 |
| 1 to 8 | 3 or 100% if less than 3 | 1 |

Errors detected during the manual audit process shall be resolved according to C.R.S. 1-7-514, and Secretary of State Rule 11. Errors discovered exceeding the error rate identified in the table above shall require escalation measures including increased audits as prescribed by the Secretary of State's office. County officials shall contact the Secretary of State's office as soon as possible if an audit detects errors above the escalation threshold.

The verification of the hand count of paper ballots shall match the totals generated from the WinEDS software as indicated in Software condition #1c. Counties shall load only the master database from the secured storage location for processing the post election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit.

*This is currently addressed by Election Rule 11.3.3*

c) Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

5) Device Security Accessibility.
Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

*This is modified and addressed by proposed Election Rule 20.5.2(c).*

**DRE Conditions (Edge2):**

1) External Power Supply Required.
Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component to accommodate a 90 minute short coming experienced by the Testing Board during testing of the device.

*This is now addressed by proposed Election Rule 20.17.6(c).*

2) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

3) Ballot/Race Conditions Simulation.
Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

4) V-VPAT Paper Record Shall Be Handled per Rule 11.6.
   a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.

      *This is now addressed by proposed Election Rule 20.6.3 and 20.11.3.*

   b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

      *This is now addressed by proposed Election Rule 20.17.5(a)(2).*

5) V-VPAT Security.
   The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

   *This is now addressed by proposed Election Rule 20.11.1(d).*

6) Accessible Distances.
   Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer's stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4" in length. Should the counties use the DRE in the stand with a reach stick, the counties shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

   *This is currently addressed by section 1-5-704, C.R.S.*

7) Accessible Operation.
   Due to the inability of the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voter and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

   *This is now addressed by proposed Election Rule 20.17.5(a)(1).*

8) Audit Trail Information:
   a) Counties will be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

*This is now addressed by proposed Election Rule 20.17.2.*

b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software condition #1c.

*This is currently addressed by Election Rule 11.3.3*

9) Confusing Instructions to Voters.
Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

*This is now addressed by proposed Election Rule 20.20.1.*

10) Device Security Accessibility.
a) The "override.ini" file is not a VSTL-certified file, and poses potential for security threat (denial of service in particular). Due to this fact the State will require the creation of a State copy of the file to ensure change control and associated hash values are passed to the counties through the distribution of the trusted build. Should a county request a change to the State certified copy of the file, the change will be made and the State will record new hash values for the file which will then be deployed in a similar fashion as the trusted build to the counties.

*This is now addressed by proposed Election Rule 20.20.3.*

b) Devices deployed in Colorado shall require a "lockable" activate button. Voter activation by use of the activate button shall not be used in the voting environment.

*This is now addressed by proposed Election Rule 20.20.2.*

c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

*This is modified and addressed by proposed Election Rule 20.5.2(c).*

**DRE Conditions (Edge2plus):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is now addressed by proposed Election Rule 20.3.3.*

2) Ballot/Race Conditions Simulation.
Additional County testing shall be required to accommodate ballots with conditions from each election. This shall include ordering a complete set of at least 4 ballots of each style that contains the prescribed design for that election. County officials shall mark each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly. All ballots in this detail shall be "marked" using the DRE device as applicable for similar testing.

*This condition is unnecessary. The goal of the pretest is to ensure that all available positions are properly counted when marked correctly. This purpose is accomplished by current Election Rule 11.3.2. Moreover, currently the logic and accuracy test must be conducted in public in accordance with current Election Rule 11.3.2(c), which enhances transparency in elections more than an internal test of 4 ballots.*

3) V-VPAT Paper Record Shall Be Handled per Rule 11.6.
   a) Prescribed paper record is of the thermal type and requires special storage conditions to avoid legibility degradation. Counties shall follow the requirements for handling according to Secretary of State Rule 11 and 43.

      *This is now addressed by proposed Election Rule 20.6.3 and 20.11.3.*

   b) Election judges are required to perform the "Printer Test" in between paper changes and verify with one additional judge that the paper has been loaded correctly and is printing according to design which ensures that all machines will have paper records for each vote cast.

      *This is now addressed by proposed Election Rule 20.17.5(a)(2).*

4) V-VPAT Security.
The V-VPAT device provides no assurance that it cannot accommodate other devices, and/or the device is a standard communication port. This connection between the V-VPAT and the DRE unit shall be secured with tamper evident seals with proper chain of custody documentation to prevent and detect tampering.

*This is now addressed by proposed Election Rule 20.11.1(d).*

5) Accessible Distances.
Operators of the system shall be required to provide an accessible solution by operating the device on a separate table. The manufacturer's stand does not meet accessible reaches as outlined in 1-5-704. Counties shall be educated on these measurements and ensuring that the table top solution complies with the requirements. This condition could also be achieved with the use of a reach stick that is at least 4" in length. Should the counties use

the DRE in the stand with a reach stick, the counties shall ensure that a side approach by a wheelchair is possible due to the deficiencies in the knee clearance (depth and width) of the stand.

*This is currently addressed by section 1-5-704, C.R.S.*

6) Accessible Operation.
Due to the inability of the voter to pause and resume the audio text, election judges shall provide instructions specific to this fact to the voter and operations for repeating the text if text was missed, which shall include details on navigating forward and backwards through the system prompts.

*This is currently addressed by section 1-5-704, C.R.S., and will be addressed by proposed Election Rule 20.17.5(a)(1).*

7) Audit Trail Information:
   a) Counties shall be required to produce certain reports identified in C.R.S. 1-7-509 using an external process which will include at a minimum exporting result from the WinEDS software for processing by other methods.

   *This is now addressed by proposed Election Rule 20.17.2.*

   b) Counties will be required to perform additional post election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include the verification of the hand count of paper records to match the totals generated from the WinEDS software as indicated in Software condition #1c.

   *This is currently addressed by Election Rule 11.3.3.*

8) Confusing Instructions to Voters.
Due to the complicated messaging provided to voters during the V-VPAT review process, the use of the device shall require election administrators to change the wording of the review screen to properly indicate to voters that a review of the ballot is taking place.

*This is now addressed by proposed Election Rule 20.20.1.*

9) Device Security Accessibility.
   a) The "override.ini" file is not a VSTL-certified file, and poses potential for security threat (denial of service in particular). Due to this fact the State will require a State copy of the file ensuring change control is passed to the counties through the distribution of the trusted build. Should a county request a change to the State certified copy of the file, the change will be made and the State will record new hash values for the file which will then be deployed in a similar fashion as the trusted build to the counties.

*This is now addressed by proposed Election Rule 20.20.3.*

b) Devices deployed in Colorado shall require a "lockable" activate button. The voting system vendor must provide schematics and assembly drawings of the button prior to installation and use, which must be approved by the Secretary of State prior to deployment. Voter activation by use of the activate button shall not be used in the voting environment.

*This is now addressed by proposed Election Rule 20.20.2.*

c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to no more than two (2) person entry with detailed logs.

*This is modified and addressed by proposed Election Rule 20.5.2(c).*

**Insight Memory Pack Receiver Conditions (2.1.5):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on memory cartridge and memory pack reader/burner and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule20.3, 20.8, and 20.9.2(a)(3).*

**Card Activator Conditions (Version 5.0.31):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on device and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

2) Cross Compatibility
The Testing Board has determined that the Card Activator is compatible for use with either the Edge2 or Edge2plus DREs

*This condition is unnecessary.*

**HAAT Model 50 Conditions (Version 2.1.18):**

1) Intrusion Seals for Protection of Trusted Build Firmware.
Device has no provision of Trusted Build verification once installed. Counties will be required to maintain constant seals on device and will require additional seals for protection against entry points as indicated by the Secretary of State. Refer to Global Condition #5a for ensuring integrity of trusted build.

*This is addressed by proposed Election Rule 20.3, 20.8, and 20.9.2(a)(3).*

2) Cross Compatibility

The Testing Board has determined that the HAAT is compatible for use with either the Edge2 or Edge2plus DREs.

*This condition is unnecessary.*