



Notice of Public Meeting

Discussion of proposed changes to

Election Rule 43 and the Conditions for Use for certified voting equipment

I. Date, time, and location of meeting

The Secretary of State will host a meeting on **December 8, 2011 from 1:00 p.m. to 5:00 p.m.** in the Blue Spruce Conference Room on the second floor of the Secretary of State's Office at 1700 Broadway, Denver, Colorado 80290.

Please note that this is not a notice of a formal rulemaking hearing. This notice and the attached draft rules are not released as part of a formal rulemaking. Instead, this is an informal meeting in anticipation of potential future rulemaking. If this office commences formal rulemaking, a notice of rulemaking, statement of basis and purpose, and preliminary draft rules will be filed and released to the public in accordance with the State Administrative Procedure Act.¹

II. Meeting subject matter and purpose

The Secretary is considering possible amendments to the election rules² in order to improve the administration and enforcement of Colorado elections law.³ Specifically, this office will consider amendments to Election Rule 43 and revisions to the Conditions for Use for the four voting system vendors that have certified voting equipment in Colorado.

The Secretary values your feedback in our rulemaking process, and we would very much like to hear your thoughts on the potential changes that we are considering proposing. Please review and consider the attached potential rule amendments. Copies of proposed revisions to the Conditions for Use for certified voting equipment are attached. Information about how to testify at the meeting and/or provide written comments is provided below.

III. Copies of potential draft rules

A preliminary draft of the proposed rules and revised Conditions for Use for each vendor is attached. A copy is also posted on the Secretary of State's website at www.sos.state.co.us/pubs/rule_making/publicMeetings/2011/20111208Elections.html. You may also contact our office to request a paper or editable electronic copy of the draft rules for consideration at the public meeting.

¹ Section 24-4-103(3)(a), C.R.S. (2011).

² 8 CCR 1505-1.

³ Article VII of the Colorado Constitution, Title 1 of the Colorado Revised Statutes, and the Help America Vote Act of 2002 ("HAVA"), P.L. No. 107-252.

IV. Opportunity to testify and submit written comments

All interested persons will have the opportunity to testify and provide written comment concerning the proposed rule amendments. To ensure that the meeting is prompt and efficient, oral testimony may be time-limited.

You may submit written comments by mail, email, or in person to our office anytime before the meeting. If you attend the meeting, you may submit written comments to the panel as well. Additional opportunity to comment in writing may be announced at the conclusion of the meeting.

All written comments will be posted online at the Secretary of State website www.sos.state.co.us/pubs/rule_making/publicMeetings/2011/20111208Elections.html. Prior to posting online, contact information including home address, email address, and telephone number(s) will be redacted from submissions unless otherwise directed by the contributor.

V. Broadcast and audio recording of meeting

If you are unable to attend the meeting, you may listen to the live broadcast from the Blue Spruce Conference Room online at www.sos.state.co.us/pubs/info_center/audioBroadcasts.html. After the meeting, visit the same website and click on “archived recordings” to access an audio recording of the meeting.

VI. Office contact

If you have any questions or would like to submit written comments, please contact Andrea Gyger with the Elections Division at andrea.gyger@sos.state.co.us or (303) 894-2200 ext. 6329.

VII. Date of notice

November 9, 2011.

**Preliminary Draft of Potential Rules
for Consideration at the December 8, 2011 Public Meeting**

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

November 9, 2011

Disclaimer:

This draft is not released as part of a formal rulemaking. If this office commences official rulemaking, a notice of rulemaking, statement of basis and purpose, and preliminary draft rules will be filed and released to the public in accordance with the State Administrative Procedure Act.¹

This preliminary draft of possible rules is provided for consideration at the following public meeting:

Date/time: December 8, 2011 from 1:00 p.m. to 5:00 p.m.
Location: Secretary of State's Office
Blue Spruce Conference Room
1700 Broadway, Second floor
Denver, Colorado 80290.

If you have questions or concerns please contact:

Andrea Gyger – Legal Specialist
Phone: (303) 894-2200 x6329
Email: Andrea.Gyger@sos.state.co.us

Proposed additions to the current rules are reflected in SMALL CAPS.

Proposed deletions from current rules are shown in ~~stricken type~~.

Annotations may be included.

1 Rule 43 would be amended as follows:

2 **Rule 43. County Security Procedures**

3 43.1 Definitions

4 43.1.1 ~~“Chain of custody-CHAIN-OF-CUSTODY log” shall, for the purposes of this rule~~ means a
5 written record that shows that the equipment and all associated data are secured
6 according to these procedures and in the documented control of an employee or deputized
7 election judge through the entire time of ownership by the jurisdiction.

8 43.1.2 ~~“Continuous video-VIDEO security surveillance recording” shall, for the purposes of this~~
9 ~~rule,~~ means video monitoring by a device which continuously records a designated
10 location. Alternatively, this definition may be met by the use of a “non-continuous”
11 recording, provided that a device is used which samples the functionality of the video
12 recorder without interruption, evaluates the detector response at least once every 15

¹ Section 24-4-103(3)(a), C.R.S. (2011).

1 seconds, and computes and records the average value at least every 60 seconds, except
2 during allowable periods of calibration.

3 43.1.3 “DRE” means a direct recording electronic voting device. A DRE is a voting device that
4 records votes by means of a ballot display provided with mechanical or electro-optical
5 components or an audio ballot that can be activated by the voter; that processes data by
6 means of a computer program; and that records voting data and ballot images in memory
7 components or other media. The device may produce a tabulation of the voting data
8 stored in a removable memory component and as printed copy. The device may also
9 provide a means for transmitting individual ballots or vote totals to a central location for
10 consolidating and reporting results from remote sites to the central location.

11 43.1.4 “Employee” ~~shall, for the purposes of this rule,~~ means all full-time, part-time, permanent,
12 and contract employees of the county who have had a criminal history check conducted
13 in accordance with Rule 11.2 and are deputized by the county clerk and recorder to
14 prepare or maintain the voting system or election setup materials, staff the counting
15 center and who have any access to the electromechanical voting systems or electronic
16 vote tabulating equipment.

17 43.1.5 “Removable card or cartridge” ~~shall, for the purposes of this rule,~~ means ~~all~~ ANY
18 programming cards or cartridges, except A voter activation cards, that stores firmware,
19 software, or data.

20 43.1.6 “SEAL” MEANS A SERIAL-NUMBERED TAMPER-EVIDENT DEVICE THAT INDICATES WHEN
21 IT HAS BEEN BROKEN OR REMOVED.

22 43.1.67 “Trusted Build” means the write-once installation disk or disks for software and firmware
23 for which the Secretary of State or his/her agent has established the chain of evidence to
24 the building of a disk, which is then used to establish and/or re-establish the chain of
25 custody of any component of the voting system which contains firmware or software.
26 The trusted build is the origin of the chain of evidence for any software and firmware
27 component of the voting system.

28 43.2 ~~Pursuant to section 1-5-616(5), C.R.S., each county shall file with the Secretary of State a~~
29 ~~security plan that meets or exceeds the standards set forth in this rule. The plan filed with the~~
30 ~~Secretary of State in accordance with this rule shall provide a point by point detailed response~~
31 ~~with a proposed solution to each of the requirements set forth in this rule. ANNUAL SECURITY~~
32 ~~PLAN. IN ACCORDANCE WITH SECTION 1-5-616(5), C.R.S., A SECURITY PLAN MUST BE~~
33 ~~SUBMITTED TO THE SECRETARY OF STATE ANNUALLY AND NO LATER THAN 60 DAYS PRIOR TO~~
34 ~~THE FIRST ELECTION IN WHICH THE SECURITY PLAN PROCEDURES WILL BE USED. THE PLAN~~
35 ~~MUST, AT A MINIMUM, INCLUDE THE FOLLOWING:~~

36 ~~43.3 The county shall file security procedures annually no later than sixty (60) days prior to the first~~
37 ~~election in which the procedures will be used.~~

38 ~~43.4 If no changes have occurred since the last security procedures filed, the county shall file a~~
39 ~~statement to that effect.~~

40 ~~43.5 Revisions to previously filed security procedures shall clearly state which part of the procedures~~
41 ~~previously filed have been revised.~~

1 ~~43.6~~ Each designated election official county may change the security procedures within sixty (60)
2 days of an election as a result of an emergency situation or other unforeseen circumstance, and
3 document any changes. The county designated election official shall file any revisions with the
4 Secretary of State within five (5) days of the change.

5 ~~43.7~~ If, pursuant to section 1-5-616(5)(b), C.R.S., the Secretary of State is unable to complete its
6 review, the procedures or revisions shall be temporarily approved until such time as the review is
7 completed. The Secretary of State shall notify the county of temporary approval.

8 *(Current rules 43.3-43.7 would be amended and relocated as rule 43.4)*

9 ~~43.8~~ Security Procedures shall at a minimum include, if applicable:

10 ~~43.8.1~~43.2.1 General Requirements:

11 a. ~~At all times removable memory cards and cartridges shall be handled in a secure manner~~
12 ~~as follows. When not sealed in voting machines, all removable cards and cartridges shall~~
13 ~~be transferred and stored in secure containers with at least one tamper evident seal with~~
14 ~~printed serial numbers. The integrity and serial number of each seal shall be verified by~~
15 ~~election judges or county personnel at shipping and receiving locations.~~

16 (A)~~b~~: All documentation of seals, chain of custody, and other documents related to the
17 transfer of equipment between parties shall be maintained on file by the county
18 clerk and recorder and is subject to inspection by the Secretary of State.

19 (B)~~e~~: The chain of custody for each voting device must be maintained and documented
20 throughout ownership or leasing of the device by the county clerk and recorder.

21 (C)~~d~~: Only deputized clerks, election judges, or canvass board members sworn under
22 oath are allowed to handle ballots, which include V-VPAT records.

23 (D)~~e~~: ~~No additional~~ ADDITIONAL or modified software developed by the Vendor MAY
24 ~~that is not specifically listed on the Secretary of State's certificate and verified~~
25 ~~against the state trusted build shall be installed on any component of the voting~~
26 ~~system ONLY IF THE SOFTWARE IS SPECIFICALLY LISTED ON THE SECRETARY OF~~
27 ~~STATE'S CERTIFICATE AND VERIFIED AGAINST THE STATE TRUSTED BUILD.~~
28 ~~Nothing in this rule shall preclude the use of commercial off the shelf software~~
29 ~~COMMERCIAL OFF-THE-SHELF SOFTWARE, provided that the COTS software is~~
30 ~~included in the certified list of services and executables for the certified voting~~
31 ~~systems.~~

32 (E)~~f~~: Any form or log containing "date" means to note the month, calendar day, year,
33 hour, minute, and whether the time is a.m. or p.m.

34 ~~43.8.2~~43.2.2 Physical Locking Mechanisms and Seals. THE COUNTY MUST RECORD THE
35 SERIAL NUMBER OF EVERY SEAL ON THE APPROPRIATE CHAIN-OF-CUSTODY LOG. TWO
36 INDIVIDUALS MUST VERIFY THE SERIAL NUMBER AND SIGN THE LOG. IF A SEAL IS
37 INACCESSIBLE AND CANNOT BE REMOVED, THEN IT IS NOT NECESSARY TO VERIFY THAT
38 SEAL SERIAL NUMBER.

1 (A)a. DREs. All DRE voting devices shall ~~have industry standard, commercial off the~~
2 ~~shelf tamper evident seals with printed, unique serial numbers affixed as follows~~
3 BE SEALED TO MEET THE FOLLOWING REQUIREMENTS:

4 (1)i. A seal shall be placed over any removable card or cartridge that is
5 inserted into the unit, or over the slot or door covering the card or
6 cartridge.

7 (2)ii. A seal is to be placed over any removable card SLOT or cartridge slot
8 when no card or cartridge is inserted into the unit.

9 (3)iii. ~~Tamper evident, numbered seals shall be affixed across the seam at~~
10 ~~which the two sides of the case of the electronic components of the~~
11 ~~voting unit join, with at least one seal for each of the four sides of the~~
12 ~~device; except in the instances where the hash value (MD5 or SHA-1) of~~
13 ~~the firmware or software can be displayed or printed by the device as~~
14 ~~verified by the State Certification process. In such cases, additional seals~~
15 ~~for the case are not required. Officials shall produce documentation of~~
16 ~~the verification of the hash value during Hardware Diagnostics Testing,~~
17 ~~Pre-Election testing and prior to the Post Election Audit as required in~~
18 ~~Rule 11~~ IF THE FIRMWARE OR SOFTWARE HASH VALUE (MD5 OR SHA-1)
19 CANNOT BE VERIFIED, THE COUNTY MUST SEAL THE DRE CASE WITH A
20 SEAL THAT ENSURES THE INTEGRITY OF THE ELECTRONIC COMPONENTS
21 CONTAINED INSIDE. SEALS SHALL BE USED AT EITHER THE SEAMS OF THE
22 CASE OR AT KEY ENTRY POINTS SUCH AS SCREW ACCESS POINTS.

23 (4)iv. If the voting device contains one or more slots for a flash memory card,
24 THE COUNTY SHALL AFFIX a seal ~~shall be affixed~~ over each flash card or
25 each flash card slot, door, or access panel.

26 (5)v. These same procedures also apply to the Judge's Booth Controller (JBC)
27 unit for the Hart InterCivic System.

28 (6)vi. ~~All seals are to be verified by two~~TWO employees or election judges
29 MUST VERIFY ALL SEALS.

30 (B)b. V-VPATs. ~~all~~ALL V-VPAT units shall be sealed upon verification of no votes
31 having been cast on the paper record prior to being attached to a specific voting
32 device. Seals must be verified as being intact by at least two election judges
33 prior to the start of voting, and at the close of voting. V-VPAT records shall
34 either remain in the V-VPAT canister, or be sealed and secured in a suitable
35 device for protecting privacy or as described in ~~Election~~ Rule 11.

36 (C)e. Remote or Central-count Optical Scanners. Optical scanners used in a remote or
37 central tabulating location shall ~~have tamper evident seals as follows~~ MEET THE
38 FOLLOWING SEAL REQUIREMENTS:

39 (1)i. A seal ~~is to~~ MUST be placed over each card or cartridge inserted into the
40 unit, or over any door or slot containing the card or cartridge.

1 (2)ii. A seal ~~is to~~ MUST be placed over each empty card or cartridge slot or
2 door covering the area where the card or cartridge is inserted.

3 (3)ii. Prior to the start of voting and after the close of voting, TWO EMPLOYEES
4 OR ELECTION JUDGES MUST VERIFY THAT all seals are ~~to be verified as~~
5 ~~being intact by two employees or election judges.~~

6 (D)d. Memory Cards/Cartridges. ~~Each removable card or cartridge shall have a~~
7 ~~permanent serial number assigned and securely affixed to it. The manufacturer~~
8 ~~assigned serial number may be utilized for this purpose.~~

9 e. ~~The county clerk and recorder shall maintain a written or electronic log that~~
10 ~~records which card or cartridge and which seal is assigned to each voting unit.~~
11 ~~The Any breach of control over a card/cartridge or door or slot for a~~
12 ~~card/cartridge before an election shall require that the county clerk and recorder~~
13 ~~be notified and follow the procedures specific to the incident as described in~~
14 ~~section 43.8.11 of this Rule.~~

15 (1) THE COUNTY MUST ASSIGN AND SECURELY AFFIX A PERMANENT SERIAL
16 NUMBER TO EACH REMOVABLE CARD OR CARTRIDGE. THE
17 MANUFACTURER ASSIGNED SERIAL NUMBER MAY BE USED FOR THIS
18 PURPOSE.

19 (2) THE COUNTY MUST HANDLE REMOVABLE MEMORY CARDS AND
20 CARTRIDGES IN A SECURE MANNER AT ALL TIMES. ANY REMOVABLE
21 CARD AND/OR CARTRIDGE THAT IS NOT SEALED IN A VOTING MACHINE
22 MUST BE TRANSFERRED AND STORED IN A SECURE CONTAINER WITH AT
23 LEAST ONE SEAL. THE SERIAL NUMBER OF EACH SEAL SHALL BE
24 VERIFIED BY ELECTION JUDGES OR COUNTY PERSONNEL IN THE CHAIN-
25 OF-CUSTODY LOGS UPON DELIVERY AND RECEIPT.

26 (3) THE COUNTY CLERK AND RECORDER MUST MAINTAIN A WRITTEN OR
27 ELECTRONIC LOG TO RECORD CARD OR CARTRIDGE SEAL SERIAL
28 NUMBERS AND TRACK SEALS FOR EACH VOTING UNIT. THE COUNTY
29 CLERK AND RECORDER MUST BE NOTIFIED IF CONTROL OF A
30 CARD/CARTRIDGE OR DOOR OR SLOT FOR A CARD/CARTRIDGE IS
31 BREACHED BEFORE AN ELECTION, AND HE/SHE MUST FOLLOW THE
32 PROCEDURES SPECIFIC TO THE INCIDENT OUTLINED IN RULE 43.2.11.

33 ~~43.8.343.2.3~~ Individuals With Access to Keys, Door Codes, and Vault Combinations

34 (A)~~43.8.3.1~~ FOR EMPLOYEES WITH ACCESS TO AREAS ADDRESSED IN RULE 43.2.3(C),
35 THE COUNTY MUST ~~Counties are required to state~~ the EMPLOYEES' TITLES
36 ~~positions~~ and THE dates of CBI background ~~check~~ CHECKS. ~~for employees with~~
37 ~~access to the areas addressed in this Rule 43.8.3.~~

38 (B)~~43.8.3.2~~ ~~For all counties,~~ THE COUNTY MUST CHANGE ALL ~~use of~~ keypad door
39 codes or locks, vault combinations, computer and server passwords, encryption
40 key codes, and administrator passwords ~~shall be changed~~ at least once per
41 calendar year prior to the first election of the year.

1 (C) EMPLOYEE ACCESS

2 (1) THE COUNTY MAY GRANT EMPLOYEES ACCESS ~~Only employees may be~~
3 ~~given access to such~~ THE codes, combinations, passwords, and encryption
4 keys DESCRIBED IN THIS RULE 43.2.3, ~~pursuant to~~ IN ACCORDANCE WITH
5 the following limitations: ~~Counties may request a variance from the~~
6 ~~Secretary of State for the requirements set forth in this Rule 43.8.3 only~~
7 ~~in extreme circumstances.~~

8 ~~43.8.3.3 The requirements for an employee to be given access to a code, combination,~~
9 ~~password, or encryption key are as follows:~~

10 (A) ~~a.~~ Access to the code, combination, password, or encryption key
11 for the storage area for voting equipment and the mail-in ballot
12 counting areas shall be restricted to employees as defined in
13 43.1.4.

14 (B) ~~b.~~ Access to the code, combination, password, or encryption key
15 for the mail-in ballot storage area and counting room or
16 tabulation workstations shall be restricted to ten ~~(10)~~ employees
17 as defined in 43.1.4.

18 (C) ~~c.~~ Except for emergency personnel, no other individuals shall be
19 present in these locations unless supervised by one or more
20 employees as defined in Rule 43.1.4.

21 (I) ~~i.~~ Each individual who has access to the central election
22 management system or central tabulator shall have their
23 own unique username and password. No individual
24 shall use any other individual's username or
25 password. Shared accounts shall be prohibited.

26 (II) ~~ii.~~ The county shall maintain a log of each person who
27 enters the ballot storage room, including the person's
28 name, signature, and date and time of entry. If access to
29 the ballot storage room is controlled by use of key card
30 or similar door access system that is capable of
31 producing a printed paper log including the person's
32 name and date and time of entry, such a log shall meet
33 the requirements of this rule.

34 (2) IN EXTREME CIRCUMSTANCE, THE COUNTY MAY REQUEST AND THE
35 SECRETARY OF STATE MAY GRANT EXEMPTION FROM THE
36 REQUIREMENTS OUTLINED IN RULE 43.2.3(C)(1).

37 (D) ~~43.8.3.4~~ Computer room access shall be limited to employees and election judges
38 only, and the delivery of ballots between the preparation room and computer
39 room shall be performed by messengers or runners wearing distinguishing
40 identification.

41 43.8.43.2.4 Temperature-controlled Storage.

1 ~~43.8.4.1 Counties~~ THE COUNTY shall attest to the temperature-control settings used with
2 the following components of a voting system. Information submitted to the
3 Secretary of State shall indicate the specifics for each type of component, as well
4 as the specific environment used, which may include, but is not limited to
5 controlled offices, controlled vaults, and controlled warehouses. The settings for
6 temperature control must be at least the following:

7 (A)~~a.~~ Servers and Workstations. Servers and workstations shall be maintained in a
8 temperature-controlled environment. Maximum temperature shall at no time
9 exceed 90 degrees ~~fahrenheit~~ FAHRENHEIT.

10 (B)~~b.~~ DREs. DREs shall be maintained in a temperature-controlled environment. The
11 temperature settings shall be maintained at a minimum of ~~60~~ 50 degrees
12 ~~fahrenheit~~ FAHRENHEIT and a maximum of 90 degrees ~~fahrenheit~~ FAHRENHEIT.

13 (C)~~c.~~ Optical Scanners. Optical scanners shall be maintained in a temperature-
14 controlled environment. The temperature settings shall be maintained at a
15 minimum of 50 degrees ~~fahrenheit~~ FAHRENHEIT and a maximum of 90 degrees
16 ~~fahrenheit~~ FAHRENHEIT.

17 (D)~~d.~~ V-VPAT Records. In addition to the requirements set forth in Rule 11, V-VPAT
18 records shall be maintained in a temperature-controlled environment. The
19 temperature settings shall be maintained at a minimum of 50 degrees ~~fahrenheit~~
20 FAHRENHEIT and a maximum of ~~80~~ 90 degrees ~~fahrenheit~~ FAHRENHEIT. V-
21 VPAT records shall also be maintained in a dry environment, with storage at
22 least ~~4~~ FOUR inches above the finished floor, for a period of 25 months following
23 the election. The humidity of the environment shall not exceed 80% humidity for
24 a period of more than 24 hours. V-VPAT records shall be stored in a manner that
25 prevents exposure to light, except as necessary during recounts and audits.

26 (E)~~e.~~ Paper Ballots. Paper ballots shall be maintained in a dry, humidity-controlled
27 environment. The humidity of the environment shall not exceed 80% humidity
28 for a period of more than 24 hours. Additionally, paper ballots shall be stored at
29 least 4 inches above the finished floor, for a period of ~~twenty five (25)~~ months
30 following the election.

31 (F)~~f.~~ Video Data Records. Video data records shall be maintained in a dry,
32 temperature-controlled environment. The humidity of the environment shall not
33 exceed 80% humidity for a period of more than 24 hours. Temperature settings
34 shall be maintained at a minimum of ~~40~~ 50 degrees ~~fahrenheit~~ FAHRENHEIT and
35 a maximum of ~~80~~ 90 degrees ~~fahrenheit~~ FAHRENHEIT. Additionally, video data
36 records shall be stored at least 4 inches above the finished floor, for a period of
37 ~~twenty five (25)~~ months following the election.

38 ~~43.8.5~~ 43.2.5 Security Cameras or Other Surveillance

39 (A)~~43.8.5.1~~ Unless otherwise instructed, ~~continuous~~ video security surveillance
40 recordings of specified areas shall be made beginning at least ~~sixty (60)~~ days
41 prior to the election and continuing through at least ~~thirty (30)~~ days after the
42 election, unless there is a recount or contest. THE RECORDING SYSTEM SHALL
43 ENSURE THAT RECORDS ARE NOT WRITTEN OVER WHEN THE SYSTEM IS FULL.

1 THE RECORDING SYSTEM SHALL PROVIDE A METHOD TO TRANSFER THE VIDEO
2 RECORDS TO A DIFFERENT RECORDING DEVICE OR TO REPLACE THE RECORDING
3 MEDIA. IF REPLACEABLE MEDIA IS USED THEN THE COUNTY SHALL PROVIDE A
4 PROCESS THAT ENSURES THAT THE MEDIA IS REPLACED OFTEN ENOUGH TO
5 PREVENT PERIODS WHEN RECORDING IS NOT AVAILABLE. If a recount or contest
6 occurs, the recording shall continue through the conclusion of all such activity.
7 The following are the specific minimum requirements:

8 (1)~~a.~~ ~~Counties~~—IF THE COUNTY HAS 50,000 OR MORE REGISTERED VOTERS,
9 THEN THE COUNTY ~~over 50,000 registered voters~~ shall make ~~continuous~~
10 video security surveillance recordings of the following areas:

11 (A)~~i.~~ All areas in which election software is used, including but not
12 limited to programming, downloading memory cards, uploading
13 memory cards, tallying results, and results reporting.

14 (B)~~ii.~~ All areas used for processing mail-in ballots, including but not
15 limited to areas used for Signature Verification, tabulation, or
16 storage of voted ballots beginning at least ~~thirty five (35)~~ days
17 prior to the election and continuing through at least ~~thirty (30)~~
18 days after the election, unless there is a recount or contest. If a
19 recount or contest occurs, the recording shall continue through
20 the conclusion of all such activity.

21 (C)~~iii.~~ The storage area for all voting equipment.

22 (2)~~b.~~ IF THE COUNTY HAS LESS THAN ~~Counties under~~ 50,000 registered voters
23 THEN THE COUNTY shall make ~~continuous~~ video security surveillance
24 recordings of ~~the following areas~~:

25 ~~i.~~ ~~ALL~~ ALL areas in which election software is used, including but
26 not limited to programming, downloading memory cards,
27 uploading memory cards, tallying results, and results reporting.

28 ~~43.8.643.2.6~~ 43.8.643.2.6 Equipment Maintenance Procedures.

29 ~~43.8.6.1~~ In addition to the requirements for voting systems specified in Rule 11, the
30 following minimum standards shall be adhered to:

31 (A)~~a.~~ All equipment shall be stored throughout the year with ~~serially numbered,~~
32 ~~tamper evident~~ seals over the memory card slots for each device. The county
33 shall maintain a log of the seals used for each device consistent to the logs used
34 for tracking Election Day seals.

35 (B)~~b.~~ For equipment being sent to the vendor for offsite repairs/replacements, the
36 county must maintain a log file for the device that shall contain the following:
37 the model number, serial number, and the type of device; the firmware version;
38 the software version (as applicable); date of submission to the vendor.

39 (C)~~c.~~ For equipment receiving maintenance on-site by the vendor, the county shall
40 verify that a CBI background check has been conducted on all vendor personnel

1 with access to any component of the voting system. CBI information shall be
2 updated and maintained on file annually. Additionally, the vendor's
3 representative shall be escorted at all times by an employee while on-site. At no
4 time shall the voting system vendor have access to any component of the voting
5 system without supervision by an employee.

6 (D)~~e~~. Upon completion of any maintenance, the county shall verify or reinstate the
7 trusted build and conduct a full acceptance test of equipment that shall, at a
8 minimum, include the Hardware Diagnostics test, as indicated in Rule 11, and
9 conduct a mock election in which an employee shall cast a minimum of FIVE ~~ten~~
10 ~~(10)~~ ballots on the device to ensure tabulation of votes is working correctly. All
11 documentation of results of the acceptance testing shall be maintained on file
12 with the specific device.

13 (E)~~e~~. The Secretary of State ~~shall be required to~~ MAY inspect ~~the counties'~~A COUNTY'S
14 maintenance records on a randomly selected one percent ~~(1%)~~ of all voting
15 devices in possession of the counties throughout the state in even-numbered
16 years, and to inspect the maintenance records on a randomly selected five percent
17 ~~(5%)~~ of all voting devices in possession of the counties throughout the state in
18 odd-numbered years.

19 ~~43.8.743.2.7~~ Transportation of Equipment, MEMORY CARDS, Ballot Boxes, and Ballots

20 (A)~~43.8.7.1~~ ~~Counties are required to~~ THE COUNTY SHALL submit detailed plans to the
21 Secretary of State prior to an election regarding the transportation of equipment
22 and ballots both to remote voting sites and back to the central elections office or
23 storage facility. While transportation of equipment may be handled in a
24 multitude of methods, the following standards shall be followed when
25 transporting voting equipment to the voting location:

26 (1)~~a~~. Transportation by County Personnel. County personnel shall at all times
27 display a badge or other identification provided by the County. Two ~~(2)~~
28 signatures and date of employees shall be required at the departure location
29 verifying that the equipment, including memory card or cartridge, is sealed to
30 prevent tampering. Upon delivery of equipment, at least two ~~(2)~~ employees
31 or election judges shall verify that all seals are intact and that the serial
32 numbers on the seals agree with those on the ~~seal-tracking~~ CHAIN-OF-
33 CUSTODY log, and sign and date the ~~seal-tracking~~ CHAIN-OF-CUSTODY log.
34 If there is any evidence of possible tampering with a seal, or if the serial
35 numbers do not agree, they shall immediately notify the county clerk and
36 recorder who shall follow the procedures specific to the incident as described
37 in ~~section 43.8.11 of this~~ Rule 43.2.11.

38 (2)~~b~~. Transportation by Election Judges. Election judges that are receiving
39 equipment from county personnel shall inspect all components of voting
40 devices and verify the specific numbers by signature and date on the ~~seal-~~
41 ~~tracking~~ CHAIN-OF-CUSTODY log for the device. The election judge receiving
42 the equipment shall request two ~~(2)~~ election judges at the voting location to
43 inspect the devices and to sign and date the ~~seal-tracking~~ CHAIN-OF-CUSTODY
44 log indicating that all seals are intact and that the serial numbers on the seals
45 agree with those on the seal-tracking log. If there is any evidence of possible

1 tampering with a seal, or if the serial numbers do not agree, they shall
2 immediately notify the county clerk and recorder who shall follow the
3 procedures specific to the incident as described in ~~section 43.8.11 of this~~
4 Rule 43.2.11.

5 (3)e. Transportation by Contract. ~~Counties~~—A COUNTY electing to contract the
6 delivery of equipment to remote voting locations shall perform CBI
7 background checks on the specific individuals who will be delivering the
8 equipment. Two ~~(2)~~ employees or election judges shall verify, sign, and date
9 the ~~seal-tracking~~ CHAIN-OF-CUSTODY log upon release of the equipment to
10 the ~~individuals~~ INDIVIDUAL(S) delivering the equipment. Two ~~(2)~~ other
11 employees or election judges shall verify, sign, and date the ~~seal-tracking~~
12 CHAIN-OF-CUSTODY log after the equipment has been delivered, and prior to
13 the opening of the polls. If there is any evidence of possible tampering with
14 a seal, or if the serial numbers do not agree, they shall immediately notify the
15 county clerk and recorder who shall follow the procedures specific to the
16 incident as described in ~~section 43.8.11 of this~~ Rule 43.2.11.

17 (B)~~43.8.7.2~~ The following standards shall be followed when transporting voting
18 equipment TO AND from the voting location:

19 (1)~~a.~~ If memory cards or cartridges are to be removed from voting devices at
20 remote voting locations, the following procedures are to be followed:

21 (A)~~i.~~ Before removing a memory card or cartridge, two ~~(2)~~ election
22 judges shall inspect and verify that all seals on the device are
23 intact and that the serial numbers on the seals agree with those
24 listed on the ~~seal-tracking~~ CHAIN-OF-CUSTODY log. Both
25 election judges shall sign and date the ~~seal-tracking~~ CHAIN-OF-
26 CUSTODY log prior to breaking the seal. If there is any evidence
27 of possible tampering with a seal, or if the serial numbers do not
28 agree, they shall immediately notify the county clerk and
29 recorder who shall follow the procedures specific to the incident
30 as described in ~~section 43.8.11 of this~~ Rule 43.2.11.

31 (B)~~ii.~~ Election judges shall place the memory cards or cartridges in a
32 sealable transfer case that shall be sealed with at least one ~~(1)~~
33 seal. Additional seal logs shall be maintained for the transfer
34 case of the memory cards or cartridges.

35 (C)~~iii.~~ Election judges shall place new seals over the empty memory
36 card/cartridge slot and/or door and document the seal numbers
37 used.

38 (D)~~iv.~~ At least two ~~(2)~~ county personnel or election judges shall
39 accompany the transfer case containing the memory
40 card/cartridge to the drop off location. Seal integrity and serial
41 numbers will be verified, and logs will be signed and dated by
42 election judges receiving the equipment. If there is any evidence
43 of possible tampering with a seal, or if the serial numbers do not
44 agree, the county personnel or election judges shall immediately

1 notify the county clerk and recorder who shall follow the
2 procedures specific to the incident as described in ~~section~~
3 ~~43.8.11 of this Rule~~ 43.2.11.

4 (E)~~v.~~ County personnel or election judges transporting secured voting
5 equipment must maintain ~~chain of custody~~ CHAIN-OF-CUSTODY
6 logs ~~and seal tracking logs~~. If there is any evidence of possible
7 tampering with a seal, or if the serial numbers do not agree, they
8 shall immediately notify the county clerk and recorder who shall
9 follow the procedures specific to the incident as described in
10 ~~section 43.8.11 of this Rule~~ 43.2.11.

11 (2)~~b.~~ If devices are to be delivered with memory cards/cartridges intact, the
12 following procedures shall be followed:

13 (A)~~i.~~ Two ~~(2)~~ county personnel or election judges shall verify that all
14 seals are intact at the close of polls. Election judges shall sign
15 the ~~seal tracking~~-CHAIN-OF-CUSTODY log with such indication.
16 If there is any evidence of possible tampering with a seal, or if
17 the serial numbers do not agree, they shall immediately notify
18 the county clerk and recorder who shall follow the procedures
19 specific to the incident as described in ~~section 43.8.11 of this~~
20 Rule 43.2.11.

21 (B)~~ii.~~ At least two ~~(2)~~ county personnel or election judges shall
22 accompany the secured equipment to the drop-off location.
23 Seals will be verified, and logs will be signed and dated by the
24 county election official receiving the equipment. If there is any
25 evidence of possible tampering with a seal, or if the serial
26 numbers do not agree, they shall immediately notify the county
27 clerk and recorder who shall follow the procedures specific to
28 the incident as described in ~~section 43.8.11 of this~~ Rule 43.2.11.

29 (C)~~iii.~~ Upon confirmation that the seals are intact and bear the correct
30 numbers, the memory card or cartridge shall be removed and
31 uploaded into the central count system.

32 (D)~~iv.~~ Election judges shall secure the equipment by placing a tamper-
33 evident seal over the memory card slot and by updating the
34 documentation to reflect the new seal ~~numbers~~NUMBER(S).

35 (C) THE FOLLOWING STANDARDS APPLY TO BALLOT BOX SECURITY AND SHALL BE
36 FOLLOWED AT ALL TIMES UNLESS OTHERWISE SPECIFIED.

37 (1) ALL BALLOT BOXES THAT CONTAIN VOTED BALLOTS SHALL BE SEALED SO
38 THAT NO BALLOT CAN BE ACCESSED WITHOUT BREAKING A SEAL. ALL
39 SEALS SHALL BE RECORDED IN THE CHAIN-OF-CUSTODY LOG AND TWO
40 ELECTION JUDGES SHALL SIGN THE CUSTODY LOG TO INDICATE THAT THE
41 REQUIRED SEALS ARE INTACT.

1 (2) ALL BALLOT BOXES THAT CONTAIN VOTED BALLOTS SHALL BE
2 ACCOMPANIED BY AT LEAST ONE ELECTION JUDGE AT ALL TIMES, EXCEPT
3 WHEN THE BALLOT BOX IS LOCATED IN A VAULT OR SECURE PHYSICAL
4 LOCATION.

5 (D) BALLOTS MAY BE PICKED UP FROM POLLING PLACES AS OFTEN AS NEEDED ON
6 ELECTION DAY. COMPLETING THE CHAIN-OF-CUSTODY LOGS REQUIRED BY THIS
7 RULE FOR EACH BALLOT BOX IS SUFFICIENT TO SUBSTANTIALLY COMPLY WITH
8 THE BALLOT BOX EXCHANGE REQUIREMENTS IN SECTION 1-7-305, C.R.S.

9 *(This new rule 43.2.7(d) would replace the written plan for alternate counting method in*
10 *current Rule 27.8)*

11 43.2.8 CONTINGENCY PLANS

12 (A)~~43.8.8~~ Emergency Contingency Plans for Voting Equipment and Voting Locations

13 (1)~~43.8.8.1~~ All remote devices used in an election shall have sufficient
14 battery backup for at least two (~~2~~) hours of use. If this requirement is
15 met by reliance on the internal battery of the voting device, then the
16 county clerk and recorder shall verify that all batteries are fully charged
17 and in working order prior to the opening of polls at the voting location.
18 This requirement also can be met with the purchase of third-party battery
19 backup systems.

20 (2)~~43.8.8.2~~ In the event of a serious or catastrophic equipment failure or
21 equipment being removed from service at one or more polling locations,
22 or there is not adequate backup equipment to meet the requirements of
23 ~~Section~~ SECTION 1-5-501, C.R.S., the county clerk and recorder shall
24 ~~contact~~ NOTIFY the Secretary of State ~~for authorization to use~~ THAT
25 provisional ballots or mail-in ballots ARE BEING USED as an emergency
26 voting method.

27 (B) A SECTION ENTITLED "CONTINGENCY PLAN" MUST BE FILED WITH THE SECURITY
28 PLAN AND MUST INCLUDE THE FOLLOWING:

29 (1) EVACUATION PROCEDURES FOR EMERGENCY SITUATIONS INCLUDING
30 FIRE, BOMB THREAT, CIVIL UNREST, AND ANY OTHER EMERGENCY
31 SITUATIONS IDENTIFIED BY THE DESIGNATED ELECTION OFFICIAL;

32 (2) BACK UP PLANS FOR EMERGENCY SITUATIONS INCLUDING FIRE, SEVERE
33 WEATHER, BOMB THREAT, CIVIL UNREST, ELECTRICAL BLACKOUT,
34 EQUIPMENT FAILURE, AND ANY OTHER EMERGENCY SITUATIONS
35 IDENTIFIED BY THE DESIGNATED ELECTION OFFICIAL;

36 (3) AN EMERGENCY CHECKLIST FOR ELECTION JUDGES; AND

37 (4) A LIST OF EMERGENCY CONTACT NUMBERS PROVIDED TO ELECTION
38 JUDGES.

1 (Current rule 43.10 would be amended and relocated to this proposed new rule
2 43.2.8(b))

3 ~~43.8.9~~43.2.9 Internal Controls for the Voting System

4 (A)~~43.8.9.1~~ In addition to the access controls discussed in ~~section 43.8.3 of this Rule~~
5 43.2.1(C), ~~counties are required to~~ THE COUNTY SHALL change all passwords and
6 limit access to the following areas:

7 (1)~~a.~~ Software. All software passwords shall be changed once per calendar year
8 prior to the first election. This includes any boot or startup passwords in use,
9 as well as any administrator and user passwords and remote device
10 passwords.

11 (2)~~b.~~ Hardware. All hardware passwords shall be changed once per calendar year
12 prior to the first election. This includes any encryption keys, key card tools,
13 supervisor codes, poll worker passwords on smart cards, USB keys, tokens,
14 and voting devices themselves as it applies to the specific system.

15 (3)~~e.~~ Password Management. Access to the administrative passwords to the
16 election management software shall be limited to two (~~2~~) employees. Access
17 to passwords for all components of the election software and hardware shall
18 be limited to two (~~2~~) employees. An additional ten (~~10~~) employees may have
19 access to the administrative passwords for the software components and an
20 additional ten (~~10~~) employees may have access to the administrative
21 passwords for the hardware components of the voting system.

22 (4)~~d.~~ Internet Access. At no time shall any component of the voting system be
23 connected, directly or indirectly, to the Internet.

24 (E)~~e.~~ Modem Transmission. At no time shall any component of the voting system
25 be connected to another device except for the vote tally software, directly or
26 indirectly, by modem as allowable by the certification of the specific device.

27 (5)~~f.~~ Remote sites may use modem functions of optical scanners and DREs only
28 for the purpose of transmitting unofficial results, as permitted by the
29 Secretary of State's certification documents for the specific systems.
30 ~~Counties~~ THE COUNTY using modem devices to transmit results shall meet
31 the following requirements:

32 (A)~~i.~~ Transmissions may be used only for sending test data or
33 unofficial results; after all other steps have been taken to close
34 the polls. All summary tapes shall be printed before connecting
35 any of the machines to a modem or telephone line.

36 (B)~~ii.~~ Modems shall not be used for any programming, setup, or
37 individual ballot-casting transmissions.

38 (C)~~iii.~~ The receiving telephone number for the modem transmission
39 shall be changed at least once per calendar year prior to the first
40 election.

1 (D)iv. A maximum of six ~~(6)~~ employees shall have access to the
2 telephone number receiving the transmission. ~~Counties~~—THE
3 COUNTY shall not publish or print the receiving telephone
4 number for any election judge. To the extent possible, the
5 telephone number shall be programmed into the device and used
6 by the device in a way that is hidden from election judges and
7 voters from seeing the display of the number at any time.

8 (6)g. Authorized Employees. ~~Counties~~—THE COUNTY shall INCLUDE in their
9 security ~~plans~~ PLAN the positions and dates of CBI background checks for
10 employees with access to any of the areas or equipment set forth in this Rule.
11 Each county shall maintain a storage-facility access log that details employee
12 name, date, and time of access to the storage facility in which the software,
13 hardware, or components of any voting system are maintained. If access to
14 the storage facility is controlled by use of key card or similar door access
15 system that is capable of producing a printed paper log including the person's
16 name and date and time of entry, such a log shall meet the requirements of
17 this rule.

18 ~~43.8.10~~43.2.10 Security Training for Election Judges

19 (A)~~43.8.10.1~~ ~~Counties~~—THE COUNTY shall include in their security plan the details of
20 their security training for their election judges, which shall include the
21 anticipated time of training, location of training, and number of election
22 judges receiving the security training, as it applies to the following
23 requirements:

24 (1)a. The county shall conduct a separate training module for field technicians and
25 election judges who will be responsible for overseeing the transportation and
26 use of the voting systems, picking up supplies, and troubleshooting device
27 problems throughout the Election Day.

28 (2)b. Security training shall include the following components:

29 (A)~~i.~~ Proper application and verification of seals and ~~seal tracking~~
30 CHAIN-OF-CUSTODY logs;

31 (B)~~ii.~~ How to detect tampering with voting equipment, memory
32 cards/cartridges, or election data on the part of anyone coming in
33 contact with voting equipment, including employees, other
34 election judges, vendor personnel, or voters;

35 (C)~~iii.~~ Ensuring privacy in voting booths;

36 (D)~~iv.~~ The nature of and reasons for the steps taken to mitigate the
37 security vulnerabilities of voting systems;

38 (E)~~v.~~ V-VPAT requirements;

39 (F)~~vi.~~—Chain-of-custody requirements for voting equipment, memory
40 cards/cartridges, and other election materials;

- (G)~~vii.~~ Ballot security;
- (H)~~viii.~~ Voter anonymity; and
- (I)~~ix.~~ Recognition and reporting of security incidents.

43.8.1143.2.11 Remedies

(A)~~43.8.11.1~~ If it is detected that the seal has been broken or if there is a discrepancy between the log and the serial number of either a voting device, or a memory card or cartridge, IN A CHAIN-OF-CUSTODY LOG, the condition must be confirmed by one or more of the remaining election judges for the location. The election judges shall immediately notify the county clerk and recorder, who shall investigate AND COMPLETE AN INTERNAL INCIDENT REPORT. ~~report the incident to the Secretary of State, and follow the appropriate remedy as indicated in this rule or as directed by the Secretary of State.~~

~~43.8.11.2~~ If a seal has been broken or removed under the following conditions:

- ~~a.~~ During either the transportation, setup, opening polls, or closing polls for the device;
- ~~b.~~ Two election judges can verify the breaking or removing of the seal; and
- ~~c.~~ The chain of custody has not been broken, meaning the device has been within ownership of election judges or employees only during this time;

~~The county clerk and recorder shall instruct the election judges to complete a security incident report detailing the incident, replacing the seals, and updating the chain of custody log as appropriate.~~

~~The Security incident report shall be filed with the Secretary of State during the canvass period.~~

(B)~~43.8.11.3~~ IF THE COUNTY CLERK AND RECORDER CONDUCTS AN INVESTIGATION IN ACCORDANCE WITH RULE 43.2.11(A) AND IS UNABLE TO DETERMINE WHY A SEAL WAS BROKEN OR WHY A DISCREPANCY EXISTS IN A CHAIN-OF-CUSTODY LOG, THEN THE COUNTY CLERK AND RECORDER SHALL FILE AN INCIDENT REPORT WITH THE SECRETARY OF STATE AS SOON AS PRACTICABLE, BUT NO LATER THAN THE CLOSE OF THE CANVASS PERIOD FOR THE ELECTION. ~~If a seal has been broken or removed outside of the situation in rule 43.8.11.2, any ANY unit involved must undergo the reinstatement or verification of the trusted build. County clerk and recorders will be required to complete a security incident report. The minimum specific requirements on the remedy are as follows the following remedial actions are required if a device has been tampered with (additional requirements may be determined based on the details of the incident report):~~

- (1)~~a.~~ For instances where the trusted build hash value (MD5 or SHA-1) of the

1 firmware or software can be displayed, VERIFIED, or printed by the device as
2 verified by the State Certification process, the election official SHALL will be
3 required to document and verify that the hash value matches the documented
4 number associated with the Trusted Build for the software or firmware of
5 that device.

6 (2)b. If the evidence INDICATES THAT THE TAMPERING OCCURRED is prior to the
7 start of voting:

8 (A)i. The device shall be sealed and securely delivered to the county
9 clerk and recorder.

10 (B)ii. The county clerk and recorder or his or her designee shall
11 remove and secure the memory card following the procedures in
12 ~~section 43.8.1(a)~~ RULE 43.2.1(A). The county clerk and recorder
13 or his or her designee shall follow the State instructions for
14 installing/verifying the trusted build for the specific device. The
15 county clerk and recorder or his or her designee shall install a
16 new, secure memory card into the device, conduct a hardware
17 diagnostics test as prescribed in Rule 11, and proceed to conduct
18 a logic and accuracy test on the machine in full election mode,
19 casting at least 25 ballots on the device. All documentation of
20 testing and chain of custody shall be maintained on file for each
21 specific device.

22 (C)iii. THE COUNTY SHALL ~~Complete~~ COMPLETE the necessary seal
23 process and documentation to re-establish the chain of custody
24 for the device and new memory card.

25 (D)iv. THE COUNTY SHALL ~~Set~~ SET the machine to election mode ready
26 for a zero report.

27 (E)vi. ~~Complete necessary reports for the Secretary of State regarding~~
28 ~~the incident as soon as practicable, but prior to the close of the~~
29 ~~canvass period for the election~~ REPEALED.

30 (3)e. If the evidence INDICATES THAT THE TAMPERING OCCURRED is after votes
31 have been cast on the device but before the close of polls:

32 (A)i. The device shall be sealed and securely delivered to the county
33 clerk and recorder.

34 (B)ii. The county clerk and recorder or his or her designee shall close
35 the election on that device, and perform a complete manual
36 verification of the paper ballots (or V-VPAT ~~Records~~ RECORDS)
37 to the summary tape printed on the device that represents the
38 record of votes on the memory card.

39 (C)iii. If the totals do not match then only the paper record will be
40 accepted as the official results for that device, and the device
41 shall be re-sealed, secured and reported to the Secretary of State

1 immediately. The device shall not be used for the remainder of
2 the election unless ~~the firmware and/or software have been~~
3 ~~reformatted with~~ the trusted build HAS BEEN REINSTALLED.

4 (D)~~iv.~~ If the totals match, the memory card may be uploaded into the
5 tally software at the close of polls.

6 (E)~~v.~~ After verifying the totals, the paper records and memory card
7 shall be secured with seals and documented properly.

8 (F)~~vi.~~ A new secured memory card shall be placed in the device. The
9 county clerk and recorder or his or her designee shall follow the
10 State instructions for installing/verifying the trusted build for the
11 specific device. The county clerk and recorder or his or her
12 designee shall conduct a hardware diagnostics test as prescribed
13 in Rule 11. All documentation of testing and chain of custody
14 shall be maintained on file for each specific device.

15 (G)~~vii.~~ THE COUNTY SHALL ~~Complete~~ COMPLETE the necessary seal
16 process and documentation to establish the chain of custody for
17 the device and memory card.

18 (H)~~viii.~~ THE COUNTY SHALL ~~Set~~ SET the machine to election mode ready
19 for a zero report.

20 (I)~~ix.~~ At the conclusion of the election a full (all races) post-election
21 audit shall be conducted on the device and results reported to the
22 Secretary of State as required by Rule 11. This requirement is in
23 addition to the random selection conducted by the Secretary of
24 State.

25 (J)~~x.~~ ~~Complete necessary reports for the Secretary of State regarding~~
26 ~~the incident as soon as practicable, but prior to the close of the~~
27 ~~canvass period for the election~~ REPEALED.

28 (4)~~d.~~ If the evidence INDICATES THAT THE TAMPERING OCCURRED ~~is~~ after the
29 close of polls:

30 (A)~~i.~~ The device shall be sealed and securely delivered to the county
31 clerk and recorder.

32 (B)~~ii.~~ The county clerk and recorder or his or her designee shall
33 perform a complete manual verification of the paper ballots (or
34 V-VPAT ~~Records~~ RECORDS) to the summary tape printed on the
35 device that represents the record of votes on the memory card.

36 (C)~~iii.~~ If the totals do not match then only the paper record will be
37 accepted as the official results for that device, and the device
38 shall be re-sealed, secured and reported to the Secretary of State
39 immediately. The device shall not be used for the remainder of

1 the election unless the firmware and/or software have ~~been~~
2 ~~reformatted with~~ the trusted build REINSTALLED.

3 (D)~~iv.~~ If the totals match, the memory card may be uploaded into the
4 tally software at the close of polls.

5 (E)~~v.~~ After verifying the totals, the paper records and memory card
6 shall be secured with seals and documented properly.

7 (F)~~vi.~~ The county clerk and recorder or his or he designee shall follow
8 the State instructions for installing/verifying the trusted build for
9 the specific device and complete the necessary seal process and
10 documentation to establish the chain of custody for the device.

11 (G)~~vii.~~ During the canvass process, a full (all races) post-election audit
12 shall be conducted on the device and results reported to the
13 Secretary of State as required by Rule 11. This requirement is in
14 addition to the random selection conducted by the Secretary of
15 State.

16 (H)~~viii.~~ ~~Complete necessary reports for the Secretary of State regarding~~
17 ~~the incident prior to the close of the canvass period for the~~
18 ~~election-REPEALED.~~

19 (C)~~43.8.11.4~~ ~~Prior to the submission of certified results from the county, the county~~
20 ~~clerk and recorder shall provide a written report to the Secretary of State~~
21 ~~addressing the existence or absence of any security issues related to the~~
22 ~~implementation and operation of the voting system.~~ All county documentation
23 related to the voting system shall be available for inspection by the Secretary of
24 State for all devices used in the election.

25 ~~43.8.12~~43.2.12 Any additional physical security procedures not discussed IN THIS RULE ~~in these~~
26 ~~mandatory procedures~~ shall be submitted to the Secretary of State for approval prior to
27 the election.

28 43.93 The COUNTY ~~designated election official~~ shall submit with the security plan sample copies of all
29 referenced forms, schedules, logs, and checklists.

30 43.4 AMENDMENTS AND REVIEW OF SECURITY PLANS

31 43.4.1 IF NO CHANGES HAVE OCCURRED SINCE THE LAST SECURITY PLAN WAS FILED, THE
32 COUNTY SHALL FILE A STATEMENT TO THAT EFFECT.

33 43.4.2 REVISIONS TO A PREVIOUSLY FILED SECURITY PLAN SHALL CLEARLY STATE WHICH
34 PARTS HAVE BEEN REVISED.

35 43.4.3 THE COUNTY MAY CHANGE THE SECURITY PLAN WITHIN 60 DAYS OF AN ELECTION AS A
36 RESULT OF AN EMERGENCY SITUATION OR OTHER UNFORESEEN CIRCUMSTANCE, AND
37 DOCUMENT ANY CHANGES. THE COUNTY MUST FILE ANY REVISIONS WITH THE
38 SECRETARY OF STATE WITHIN FIVE DAYS OF THE CHANGE.

1 43.4.4 IF, UNDER SECTION 1-5-616(5)(B), C.R.S., THE SECRETARY OF STATE IS UNABLE TO
2 COMPLETE ITS REVIEW, THE SECURITY PLAN OR REVISIONS WILL BE TEMPORARILY
3 APPROVED UNTIL SUCH TIME AS THE REVIEW IS COMPLETED. THE SECRETARY OF STATE
4 WILL NOTIFY THE COUNTY OF TEMPORARY APPROVAL.

5 *(Proposed new rule 43.4 includes the amended and relocated current rules 43.3 through 43.7)*

6 ~~43.10~~ Included in the security procedures filed with the secretary of state shall be a section entitled
7 “contingency plan.” The contingency plan shall include:

8 ~~(a)~~ Evacuation procedures for emergency situations including fire, bomb threat, civil unrest,
9 and any other emergency situations identified by the designated election official;

10 ~~(b)~~ Back up plans for emergency situations including fire, severe weather, bomb threat, civil
11 unrest, electrical blackout, equipment failure, and any other emergency situations
12 identified by the designated election official;

13 ~~(c)~~ An emergency checklist for election judges; and

14 ~~(d)~~ A list of emergency contact numbers provided to election judges.

15 *(Current rule 43.10 would be amended and relocated to new rule 43.2.8(b))*

16 43.445 Lease, Loan, or Rental of Election Equipment

17 43.445.1 Nothing in this Rule ~~shall be construed to require~~ requires a county clerk to lease,
18 loan, or rent any election equipment to any municipality, special district or other local
19 jurisdiction.

20 43.445.2 A county clerk who chooses to lease, loan, or rent any certified election
21 equipment to a municipality, special district, or other local jurisdiction for use in their
22 elections shall follow at least one of the following procedures in order to maintain or
23 reestablish an acceptable chain of custody and appropriate documentation ~~pursuant to~~ IN
24 ACCORDANCE WITH Rule ~~43.8-43.2.1~~.

25 ~~(A)~~ After the certified equipment has been returned to the county clerk by the
26 applicable jurisdiction, and prior to use of the equipment in any primary, general,
27 congressional vacancy, statewide ballot issue (including recall), or special
28 election conducted by the county clerk, reinstatement or verification of the
29 trusted build, ~~pursuant to~~ IN ACCORDANCE WITH Rule ~~43.8-11.3(a)~~ 43.2.11(B)(1),
30 shall be completed.

31 ~~(B)~~ The county clerk or their deputized representative shall:

32 ~~(1)~~ Deliver the certified equipment to the jurisdiction;

33 ~~(2)~~ Witness and document the installation of the memory card(s) or
34 cartridge(s) to be used by the jurisdiction;

35 ~~(3)~~ Place one or more secure and numbered seals on the voting equipment
36 ~~pursuant to~~ IN ACCORDANCE WITH Rule ~~43.8-2-43.2.2~~. If during the

1 course of the jurisdiction's election, the designated election official
2 requires removal of a memory card or cartridge as a function of the
3 election process, the county clerk or their deputized representative shall
4 witness and document the removal and proper resealing of the memory
5 card or cartridge; and

6 (4)~~IV~~. Upon return of the equipment to the county clerk and recorder, the
7 county clerk shall verify and document that the seals are intact. If any
8 seal appears to be damaged or removed, the county clerk shall reinstall or
9 verify the trusted build in accordance with this Rule 43.

10 (C)~~e~~. The county clerk and recorder shall designate deputized county staff to be
11 stationed with the loaned certified equipment at all times while the equipment is
12 under control of the designated election official. The certified equipment shall
13 not be allowed out of the physical custody of the deputized county staff at any
14 time. The deputized county staff shall ensure that no unauthorized access occurs.

15 (D)~~d~~. ~~Pursuant to~~ IN ACCORDANCE WITH section 1-5-605.5, C.R.S., the county clerk
16 shall appoint the designated election official as a deputy for the purposes of
17 supervising the certified voting equipment. The designated election official
18 shall:

19 (1)~~I~~. Sign and submit to the county clerk and recorder an affirmation that
20 he/she will ensure the security and integrity of the certified voting
21 equipment at all times;

22 (2)~~II~~. Affirm that the use of the certified voting equipment shall be conducted
23 in accordance with Rule 43 and the specific conditions for use of the
24 certified voting equipment; and

25 (3)~~III~~. Agree to maintain all ~~chain-of-custody~~ CHAIN-OF-CUSTODY logs for the
26 voting device(s).

27 43.~~44~~5.3 Upon return of the certified voting equipment to the county clerk and recorder,
28 the county clerk ~~shall~~ IS ~~not~~ be required to verify the trusted build if the documentation
29 and chain of custody DOES NOT support the proper maintenance of the trusted build
30 software and chain of custody.

The following Conditions for Use are required for the ES&S Unity 3.0.1.1 voting system. Any deviation from the Conditions for Use could lead to significant weakness in the security, auditability, integrity, and availability of the voting system.

Definitions

1. “Testing Board” means the Colorado Department of State Elections Division.
2. “Voting Device” means a device used to record votes.

Global Conditions (applies to all components)

1. Modem and Telecommunication Devices

The voting system vendor was unable to meet or provide prerequisite FIPS 140/180 certifications as required by Rule 45.5.2.7.2. Therefore, modems and other telecommunication devices shall not be used to transmit official election results. Modems may be used to transmit unofficial election results that are clearly marked or labeled as unofficial.

2. Provisional Ballots

The county is required to implement a procedure for handling provisional ballots outside of the system, because the software is not capable of accepting only state and federal questions on a provisional ballot.

3. Abstracts

The abstracts and reports created by the software do not meet the requirements of Election Rule 41.6.3(g). Therefore the county is required to generate an abstract outside of the voting system. The reports generated by a tabulation device shall not be used for State reporting.

4. Closed Network

The county is required to affirm in its Security Plan that the voting system will only be used on a closed network.

Software Conditions (Unity 3.0.1.1)

1. System/Database/Network Security Hardening

- a. The county is required to modify the physical security of all locations that house the Unity Software because the voting system operates in a non-restricted system configuration which allows the election database to be modified by third-party software tools without detection. The county shall include their plan for complying with this condition as part of their Security Plan required by Election Rule 43.
- b. The county shall create a backup copy of the Unity database that is created immediately after the memory cards have been downloaded to the device. 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. The county shall record the chain of custody of the CD media, and the CD media shall be sealed with at least two tamper evident seals. The sealed CD media shall be stored in a

sealed or locked transfer case that is stored in a secure area. Prior to uploading any memory cards on election day, the designated election official shall load the sealed copy of the database onto the server and document that the backup master copy has been loaded on the system. After the backup copy has been loaded the CD media shall be re-secured with seals and shall be kept in a secure area

2. Logs

The county is required to maintain logs indicating the use of report printing functions within the software. Logs are also required to record hardware changes and any system property change made by either a staff member or election judge. Hardware changes include inserting or removing removable media. Logs shall be maintained in a file outside of or separate from the database. The logs shall not be accessible for review and/or modification by the user accounts on the system.

Such logs may be achieved through key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records, or any combination necessary to complete an audit of the data. The county shall include their process for meeting the requirements of this condition in their Security Plan.

3. Election Database Creation and Testing

- a. The county is required to ensure that ballots are designed and created according to state specifications.
- b. The county is required to maintain a log of changes made to any component of the system because the system logs do not accurately represent changes made within the system.

Precinct Count Scanner Conditions (M100)

1. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

2. Audit Trail Information

- a. The county is required to maintain logs to track the use of the administrator functions of the device by either election judges or county staff.
- b. The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.

3. Secrecy Sleeve

The county is required to use the system secrecy sleeve provided by ES&S for ballots with one column. For ballots with more than one column, the county shall create a secrecy sleeve to accommodate the deficiency. The secrecy sleeve created by the county shall be submitted to the Secretary of State for approval.

Central Count Scanner Conditions (M650)

1. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

2. Audit Trail Information

- a. The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.
- b. The county is required to save each batch to a zip disk.

DRE Conditions (iVotronic)

1. Audit Trail Information

The county is required to maintain logs to track the use of the administrator functions of the device by either election judges or county staff.

2. V-VPAT Security

- a. The county is required to secure the connection between the V-VPAT and the DRE unit to prevent and detect tampering because the device utilizes a standard communication port.
- b. The county shall only use the 9 inch screen because vote data can be viewed by the election judges when the 4.5 inch screen is used.
- c. The lock on the V-VPAT must be sealed with a tamper-evident seal.

3. Accessible Operation

- a. The county is required to train election judges how to give specific information to the elector for repeating audio text because the system does not allow the elector to pause and repeat audio.
- b. A headset must be provided that meets the State of Colorado specifications.

The following Conditions for Use are required for the Hart System 6.0 and System 6.2.1 voting systems. Any deviation from the Conditions for Use could lead to significant weakness in the security, auditability, integrity, and availability of the voting system.

Definitions

1. “Testing Board” means the Colorado Department of State Elections Division.
2. “Voting Device” means a device used to record votes.

Global Conditions (applies to all components)

1. Modem and Telecommunication Devices

The voting system vendor was unable to meet or provide prerequisite FIPS 140/180 certifications as required by Rule 45.5.2.7.2. Therefore, modems and other telecommunication devices shall not be used to transmit official election results. Modems may be used to transmit unofficial election results that are clearly marked or labeled as unofficial.

2. Provisional Ballots

The county is required to implement a procedure for handling provisional ballots outside of the system, because the software is not capable of accepting only state and federal questions on a provisional ballot.

3. Abstracts

The abstracts and reports created by the software do not meet the requirements of Election Rule 41.6.3(g). Therefore the county is required to generate an abstract outside of the voting system. The reports generated by a tabulation device shall not be used for State reporting.

4. Closed Network

- a. The county is required to affirm in its Security Plan that the voting system will only be used on a closed network.
- b. The use of wireless components is forbidden on the system. Any workstation or laptop that is designed with wireless communications shall have the device disabled.

5. Virus Protection

The county is required to use virus protection software which is compatible with the operating system that contains the election software.

Software Conditions (BOSS, Tally, Rally, and SERVO)

1. System/Database/Network Security Hardening

- a. The county is required to modify the physical security of all locations that house the BOSS Software because the voting system operates in a non-restricted system configuration which allows the election database to be modified by third-party software tools without detection. The county shall include their plan for complying with this condition as part of their Security Plan required by Election Rule 43.

- b. The county shall create a backup copy of the Tally database that is created immediately after the memory cards have been downloaded to the device. 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. The county shall record the chain of custody of the CD media, and the CD media shall be sealed with at least two tamper evident seals. The sealed CD media shall be stored in a sealed or locked transfer case that is stored in a secure area. Prior to uploading any memory cards on election day, the designated election official shall load the sealed copy of the database onto the server and document that the backup master copy has been loaded on the system. After the backup copy has been loaded the CD media shall be re-secured with seals and shall be kept in a secure area

2. Logs

The county is required to maintain logs indicating the use of report printing functions within the software. Logs are also required to record hardware changes and any system property change made by either a staff member or election judge. Hardware changes include inserting or removing removable media. Logs shall be maintained in a file outside of or separate from the database. The logs shall not be accessible for review and/or modification by the user accounts on the system.

Such logs may be achieved through key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records, or any combination necessary to complete an audit of the data. The county shall include their process for meeting the requirements of this condition in their Security Plan.

3. Performance Deficiencies

Counties shall ensure that hardware purchased for the system matches the specifications of the VSTL versions and not the documentation provided by Hart.

Precinct Count Scanner Conditions (eScan)

1. Protection of Trusted Build Firmware

When the integrity of an eScan's firmware has been compromised the county shall use SERVO's "Verify Device Firmware" function (under the "Device Backup and Reset" menu) to verify that the firmware is the same as the Trusted Build. The appropriate firmware integrity file, available from the Secretary of State, must be imported into SERVO before performing this function.

2. Ballot Processing

The device shall be set up so that the poll worker is required to use the override key on the back of the device in the event a ballot is rejected. A ballot page shall not be fed through the eScan until the previous ballot page has been completely scanned.

3. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

4. Secrecy Sleeve

The county is required to use the system secrecy sleeve provided by Hart for ballots with one column. For ballots with more than one column, the county shall create a secrecy sleeve to accommodate the deficiency. The secrecy sleeve created by the county shall be submitted to the Secretary of State for approval.

5. Audit Trail Information

- a. The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.
- b. Due to errors in processing and auditing information processed by the device, the device will be limited so that it can only use ballots with serial numbers.
- c. The county shall not reset the device without transferring the audit log from the device to SERVO.

Central Count Scanner Conditions (Ballot Now/Scanners)

1. Ballot Processing

Election judges 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.

2. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

3. Audit Trail Information

The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.

4. eScan

If the county uses an eScan as a central count scanner then the county is required to comply with the central count conditions and eScan precinct count scanner conditions numbered 1, 5(b), and 5(c).

DRE Conditions (eSlate)

1. Additional Power Supply Required

Counties shall purchase and make available an additional power supply for the Verifiable Ballot Option (VBO) that meets or exceeds the vendor's recommendations because the VBO did not operate for 2 continuous hours on battery power. Switching the VBO batteries within a reasonable amount of time is sufficient to fulfill this condition.

2. Protection of Trusted Build Firmware

- a. The county is required to maintain a seal on the VBO's programming connector and case. Additionally, the communications port is to be sealed when it is not installed in the eSlate case.
- b. When the integrity of an eSlate or JBC firmware has been compromised the county shall use SERVO's "Verify Device Firmware" function (under the "Device Backup and Reset" menu) to verify that the firmware is the same as the Trusted Build. The appropriate firmware integrity file, available from the Secretary of State, must be imported into SERVO before performing this function.
- c. An election official is required to change passwords on the JBC to prevent the manufacturer from accessing the device.

3. V-VPAT Printer

Election judges are required to test the V-VPAT printer between paper changes to verify that the paper was loaded correctly and is able to print a legible record.

4. Audit Trail Information

- a. The county is required to maintain logs to track the use of the administrator functions of the device by either election judges or county staff.
- b. The county shall not reset the device without transferring the audit log from the device to SERVO.
- c. 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.

5. V-VPAT Security

- a. The county is required to secure the connection between the V-VPAT and the DRE unit to prevent and detect tampering because the device utilizes a standard communication port.
- b. The lock on the V-VPAT must be sealed with a tamper-evident seal.

6. V-VPAT Truncation

Before the logic and accuracy test is conducted the county shall determine whether any candidate names will be truncated. If there is any indication of truncation and the county is unable to fix the truncation problem, then a printed notice will be provided to the voters prior to voting on the DRE.

7. Accessibility

- a. The county is required to train election judges how to give specific information to the elector for repeating audio text because the system does not allow the elector to pause and repeat audio.
- b. The county is required to provide a headset with an adjustable volume control.

DRAFT

The following Conditions for Use are required for the Premier GEMS 1-18-24 voting system. Any deviation from the Conditions for Use could lead to significant weakness in the security, auditability, integrity, and availability of the voting system.

Definitions

1. “Testing Board” means the Colorado Department of State Elections Division.
2. “Voting Device” means a device used to record votes.

Global Conditions (applies to all components)

1. Modem and Telecommunication Devices

The voting system vendor was unable to meet or provide prerequisite FIPS 140/180 certifications as required by Rule 45.5.2.7.2. Therefore, modems and other telecommunication devices shall not be used to transmit official election results. Modems may be used to transmit unofficial election results that are clearly marked or labeled as unofficial.

2. Provisional Ballots

The county is required to implement a procedure for handling provisional ballots outside of the system, because the software is not capable of accepting only state and federal questions on a provisional ballot.

3. Abstracts

The abstracts and reports created by the software do not meet the requirements of Election Rule 41.6.3(g). Therefore the county is required to generate an abstract outside of the voting system. The reports generated by a tabulation device shall not be used for State reporting.

4. Closed Network

The county is required to affirm in its Security Plan that the voting system will only be used on a closed network.

Software Conditions (GEMS 1-18-24)

1. System/Database/Network Security Hardening

- a. The county is required to modify the physical security of all locations that house the GEMS Software because the voting system operates in a non-restricted system configuration which allows the election database to be modified by third-party software tools without detection. The county shall include their plan for complying with this condition as part of their Security Plan required by Election Rule 43.
- b. The county shall create a backup copy of the GEMS database that is created immediately after the memory cards have been downloaded to the device. 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. The county shall record the chain of custody of the CD media, and the CD media shall be sealed with at least two tamper evident seals. The sealed CD media shall be stored in a

sealed or locked transfer case that is stored in a secure area. Prior to uploading any memory cards on election day, the designated election official shall load the sealed copy of the database onto the server and document that the backup master copy has been loaded on the system. After the backup copy has been loaded the CD media shall be re-secured with seals and shall be kept in a secure area

2. Logs

The county is required to maintain logs indicating the use of report printing functions within the software. Logs are also required to record hardware changes and any system property change made by either a staff member or election judge. Hardware changes include inserting or removing removable media. Logs shall be maintained in a file outside of or separate from the database. The logs shall not be accessible for review and/or modification by the user accounts on the system.

Such logs may be achieved through key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records, or any combination necessary to complete an audit of the data. The county shall include their process for meeting the requirements of this condition in their Security Plan.

Precinct Count Scanner Conditions (1.96.6)

1. Audit Trail Information

- a. The county is required to maintain logs to track the use of the administrator functions of the device by either election judges or county staff.
- b. The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.

Central Count Scanner Conditions (2.0.12)

1. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

2. Auto-Calibration Verification

The county 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.

3. Audit Trail Information

The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.

DRE Conditions (TSx 4.6.4 – C and D models)

1. V-VPAT Printer

Election judges are required to test the V-VPAT printer between paper changes to verify that the paper was loaded correctly and is able to print a legible record.

2. Accessibility

- a. The county is required to provide a solution that allows the device units to meet the accessibility requirements outlined in section 1-5-704(1)(m), C.R.S., and Rules 35.1.15, 35.1.16, and 35.1.17, because the manufacturer's stand does not meet these standards. This condition could be met with the use of a reach stick that is at least 4" in length. Should the county use the DRE in the stand with a reach stick, then the county 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.
- b. The county is required to train election judges how to give specific information to the elector for repeating audio text because the system does not allow the elector to pause and repeat audio.
- c. The privacy panels attached to the device are inadequate and therefore the county shall use either computer monitor polarized privacy screens or take additional measures to ensure that electors and judges cannot easily walk behind a voting elector.

The following Conditions for Use are required for the Sequoia WinEDS 3.1.074 voting system. Any deviation from the Conditions for Use could lead to significant weakness in the security, auditability, integrity, and availability of the voting system.

Definitions

1. “Testing Board” means the Colorado Department of State Elections Division.
2. “Voting Device” means a device used to record votes.

Global Conditions (applies to all components)

1. Modem and Telecommunication Devices

The voting system vendor was unable to meet or provide prerequisite FIPS 140/180 certifications as required by Rule 45.5.2.7.2. Therefore, modems and other telecommunication devices shall not be used to transmit official election results. Modems may be used to transmit unofficial election results that are clearly marked or labeled as unofficial.

2. Provisional Ballots

The county is required to implement a procedure for handling provisional ballots outside of the system, because the software is not capable of accepting only state and federal questions on a provisional ballot.

3. Abstracts

The abstracts and reports created by the software do not meet the requirements of Election Rule 41.6.3(g). Therefore the county is required to generate an abstract outside of the voting system. The reports generated by a tabulation device shall not be used for State reporting.

4. Closed Network

The county is required to affirm in its Security Plan that the voting system will only be used on a closed network.

Software Conditions (WinEDS 3.1.074)

1. System/Database/Network Security Hardening

- a. The county is required to modify the physical security of all locations that house the WinEDS Software because the voting system operates in a non-restricted system configuration which allows the election database to be modified by third-party software tools without detection. The county shall include their plan for complying with this condition as part of their Security Plan required by Election Rule 43.
- b. The county shall create a backup copy of the WinEDS database that is created immediately after the memory cards have been downloaded to the device. 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. The county shall record the chain of custody of the CD media, and the CD media shall be sealed with at least two tamper evident seals. The sealed CD media shall be stored in a sealed or locked transfer case that is stored in a secure area. Prior to uploading any

memory cards on election day, the designated election official shall load the sealed copy of the database onto the server and document that the backup master copy has been loaded on the system. After the backup copy has been loaded the CD media shall be re-secured with seals and shall be kept in a secure area

2. Logs

The county is required to maintain logs indicating the use of report printing functions within the software. Logs are also required to record hardware changes and any system property change made by either a staff member or election judge. Hardware changes include inserting or removing removable media. Logs shall be maintained in a file outside of or separate from the database. The logs shall not be accessible for review and/or modification by the user accounts on the system.

Such logs may be achieved through key stroke recording software, windows event log recordings, detailed video camera recordings, manually written records, or any combination necessary to complete an audit of the data. The county shall include their process for meeting the requirements of this condition in their Security Plan.

3. Trusted Build Protection

The trusted build of the WinEDS software cannot be verified once it has been installed. Therefore, the integrity of the trusted build must be protected after it has been installed on the county's computer(s). This applies to the WinEDS software and custom components of SQL server as applicable.

4. Election Database Creation and Testing

WinEDS relies heavily on an uncertified Sequoia application called BPS which typically is used for importing the ballot setup process into WinEDS. Since this program is not part of the trusted build then its use is to be restricted. Exported data from the BPS application shall not be imported into WinEDS. Data from the BPS application can be exported to a static import file format such as flat file, csv, txt, or similar which can then be imported into WinEDS using the appropriate file format. Data from WinEDS can be freely exported for import into the BPS application.

Precinct Count Scanner Conditions (Insight/Insight Plus)

1. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

2. Secrecy Sleeve

The county is required to use the system secrecy sleeve provided by Sequoia for ballots up to 14 inches. For longer ballots, the county shall create a secrecy sleeve to accommodate the deficiency. The secrecy sleeve created by the county shall be submitted to the Secretary of State for approval.

3. Audit Trail Information

The county is required to maintain logs to track the use of the administrator functions of the device by either election judges or county staff.

Central Count Scanner Conditions (400C)

1. System/Database/Network Security Hardening

The county is required to modify the physical security of all locations that house the 400C central count scanner because the voting system operates in a non-restricted system configuration which allows the election database to be modified by third-party software tools without detection. The county shall include their plan for complying with this condition as part of their Security Plan required by Election Rule 43.

2. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

3. Audit Trail Information

The county is required to include the serial number of the device on all reports regarding the use of the device. The county shall also include the serial number on all reports from the device.

DRE Conditions (Edge 2 and Edge2Plus unless otherwise noted)

1. Additional Power Supply Required

If the main power source is lost, the county shall use an additional power supply that meets or exceeds the vendor's recommendation for the component because the device was not able to run continuously for 2 hours during testing.

2. V-VPAT Printer

Election judges are required to test the V-VPAT printer between paper changes to verify that the paper was loaded correctly and is able to print a legible record.

3. V-VPAT Security

The county is required to secure the connection between the V-VPAT and the DRE unit to prevent and detect tampering because the device utilizes a standard communication port.

4. Voter Instructions

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.

5. Device Security

- a. The "override.ini" file is not a VSTL-certified file, and poses potential for security threat (denial of service in particular). The county is required to create a copy of the file for the Secretary of State 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.

- 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. [Only applicable to Edge2]
 - c. 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. [Only applicable to Edge2Plus]
6. Accessibility
- a. The county is required to provide a solution that allows the accessible device units to meet the accessibility requirements outlined in section 1-5-704(1)(m), C.R.S., and Rules 35.1.15, 35.1.16, and 35.1.17 because the manufacturer’s stand does not meet these accessibility standards. This condition could be met with the use of a reach stick that is at least 4” in length. Should the county use the DRE in the stand with a reach stick, then the county 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.
 - b. The county is required to train election judges how to give specific information to the elector for repeating audio text because the system does not allow the elector to pause and repeat audio.
 - c. The privacy panels attached to the device are inadequate and therefore the county shall use either computer monitor polarized privacy screens or take additional measures to ensure that electors and judges cannot easily walk behind a voting elector.

Insight Memory Pack Receiver Conditions (2.1.5):

1. Intrusion Seals for Protection of Trusted Build Firmware.

The county is required to maintain constant seals on memory cartridges and memory pack receiver input ports and case. The case seals shall be sufficient to ensure that the device case has not been opened enough to allow tampering with the electronic components inside of the case. Seals may be used at the seams of the case or at key points such as screw access points.

Card Activator Conditions (Version 5.0.31):

1. Intrusion Seals for Protection of Trusted Build Firmware.

The county is required to maintain constant seal(s) on the device sufficient to prevent the device from being opened without detection. Seals may be used at the seams of the case or at key points such as screw access points.

2. Cross Compatibility

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

HAAT Model 50 Conditions (Version 2.1.18):

1. Intrusion Seals for Protection of Trusted Build Firmware.

The county is required to maintain constant seal(s) on device sufficient to prevent the device from being opened without detection. Seals may be used at the seams of the case or at key points such as screw access points.

2. Cross Compatibility

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