Andrea Gyger

From: Marilyn Marks [redacted]
Sent: Sunday, December 04, 2011 10:03 PM
To: Andrea Gyger
Cc: Richard Coolidge; Scott Gessler
Subject: Rule 43 Informal comments
Attachments: Rule43PublicMeetingComments_M_Marks.pdf

Categories: Rules

Ms. Gyger,
Please find my very informal comments annotated in the attached pdf.

Please also include the following comments for consideration.

1. The proposed Rule 43 changes appear to allow a dilution of the security standards in voting systems in some areas at a time that the public is demanding more election security. For example, the removal of the need for continuous video greatly reduces the effectiveness of video security. I have personally been in a situation (as a candidate) when I discovered an unattended unlocked ballot box with 800 voted ballots, and the keys hanging from the ballot box. I could have compromised the Accu-vote machine and ballots rapidly enough to escape detection on slower still frame video systems. The area needs continuous video surveillance and constant security lighting.

   Additionally, it appears that one goal of the rule changes is to concentrate with the clerks all authority and responsibility for investigating and reporting security breaches. The result is to dilute the oversight, while reducing the chances that security incidents will be promptly reported and investigated.

2. Most importantly, the voting system security rules should address the fundamental election security requirement that no system (including the entire election processing as a "system"), may facilitate the ability to connect the voter and ballot after the ballot is cast. It appears that in some counties batching of ballots and unique style numbers in a batch are creating traceability of ballots back to voters. It also appears that unique ballot style numbers are causing problems of traceability, which can be solved with relatively simple rule-making. Election judges' oaths are insufficient to meet the state constitutional mandate for anonymous or absolute secrecy in voting.

   Th**e security of the system must not be compromised by traceable, non-anonymous ballots. All of the other security measures are rather meaningless without the guarantee of a system that complies with the state constitution for anonymous ballots. Otherwise, the elections conducted will be subject to being voided by the courts.**

If you require a more formalized comment format, please let me know.
Thank you for your consideration.
Marilyn Marks

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

Scott Gessler
Secretary of State

William A. Hobbs
Deputy Secretary of State

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 rules[2] 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.

Rule 43 would be amended as follows:

Rule 43. County Security Procedures

43.1 Definitions

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

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

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

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

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

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

43.1.5 "Removable card or cartridge" ~~shall, for the purposes of this rule,~~ means ~~all~~ ANY programming card~~s~~ or cartridge~~s~~, except A voter activation card~~s~~, that store~~s~~ firmware, software, or data.

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

43.1.~~6~~7 "Trusted Build" means the write-once installation disk or disks for software and firmware for which the Secretary of State or his/her agent has established the chain of evidence to the building of a disk, which is then used to establish and/or re-establish the chain of custody of any component of the voting system which contains firmware or software. The trusted build is the origin of the chain of evidence for any software and firmware component of the voting system.

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

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

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

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

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

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

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

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

~~43.8.1~~43.2.1 General Requirements:

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

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

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

should include watchers sworn under oath.

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

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

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

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

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

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

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

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

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

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

what does "verify" mean? How will verfication be documented?

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

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

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

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

use election judges only, as more effective oversight.

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

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

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

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

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

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

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

~~43.8.3~~43.2.3 Individuals With Access to Keys, Door Codes, and Vault Combinations

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

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

(C) EMPLOYEE ACCESS

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

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

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

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

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

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

(II)~~ii.~~ The county shall maintain a log of each person who enters the ballot storage room, including the person's name, signature, and date and time of entry. If access to the ballot storage room 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 shall meet the requirements of this rule.

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

watchers, including media observers should have access as well. Otherwise, oversight is lost at this critical point.

~~3.8.3.4~~ Computer room access shall be limited to employees and election judges only, and the delivery of ballots between the preparation room and computer room shall be performed by messengers or runners wearing distinguishing identification.

~~43.8.4~~43.2.4 Temperature-controlled Storage.

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

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

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

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

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

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

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

~~43.8.5~~43.2.5 Security Cameras or Other Surveillance

continuous video is needed. Anything else is too easy to compromise and security breaches are not detected.

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

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

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

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

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

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

continuous video recording should not be dropped.

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

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

~~43.8.6~~43.2.6 Equipment Maintenance Procedures.

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

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

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

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

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

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

require SOS mandatory inspection and do not limit his power to inspect ONLY 1 %. Some people will read "MAY" as the limit on authority to inspect.

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

~~43.8.7~~43.2.7 Transportation of Equipment, MEMORY CARDS, Ballot Boxes, and Ballots

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

make clear that ballot boxes means transfer cases, and any storage containers for ballots

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

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

"secure physical location" should be clearly defined, -- example--Saguache where ballots are kept in "vault" and "secure storage room," but many county employees and title company employees have access.

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

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

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

43.2.8 CONTINGENCY PLANS

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

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

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

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

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

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

(3) AN EMERGENCY CHECKLIST FOR ELECTION JUDGES; AND

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

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

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

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

this presumes that software passwords are required. Saguache does not have passwords on the software and therefore this would not apply.

(1)~~a.~~ Software. All software passwords shall be changed 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.

(2)~~b.~~ Hardware. All hardware passwords shall be changed 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.

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

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

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

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

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

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

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

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

(6)~~g.~~ Authorized Employees. ~~Counties~~ THE COUNTY shall INCLUDE in their security ~~plans~~ PLAN the positions and dates of CBI background checks for employees with access to any of the areas or equipment set forth in this Rule. Each county shall 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 shall meet the requirements of this rule.

~~43.8.10~~43.2.10 Security Training for Election Judges

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

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

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

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

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

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

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

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

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

(G)~~vii.~~ Ballot security;

(H)~~viii.~~ Voter anonymity~~.~~; and

(I)~~ix.~~ Recognition and reporting of security incidents.

~~43.8.11~~43.2.11 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:~~

this requirement should not be diluted.

~~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.~~

this leaves far too much discretion in hands of Clerk. Example Saguache where clerk would not allow investigation. Election judges and canvass board should have DUTY to report to Clerk and SOS.

~~.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):

this requires the clerk to determine a definition of "tampering" and whether a machine has been "tampered with." This further reduces security.

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

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

this dilutes oversight and security.
Clerks are required to analyze whether "tampering occurred," and should not be put in the position to do so.

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

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

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

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

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

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

same comments as above.
Clerk should not be sole determiner of whether to report to SOS and whether "tampering" has occurred.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

this requirement should not be removed. no reason to dilute the security measures.

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

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

43.~~9~~3 The COUNTY ~~designated election official~~ shall submit with the security plan sample copies of all referenced forms, schedules, logs, and checklists.

43.4 AMENDMENTS AND REVIEW OF SECURITY PLANS

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

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

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

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

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

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

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

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

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

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

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

43.~~11~~5 Lease, Loan, or Rental of Election Equipment

43.~~11~~5.1 Nothing in this Rule ~~shall be construed to require~~ requires a county clerk to lease, loan, or rent any election equipment to any municipality, special district or other local jurisdiction.

43.~~11~~5.2 A county clerk who chooses to lease, loan, or rent any certified election equipment to a municipality, special district, or other local jurisdiction for use in their elections shall follow at least one of the following procedures in order to maintain or reestablish an acceptable chain of custody and appropriate documentation ~~pursuant to~~ IN ACCORDANCE WITH Rule ~~43.8~~ 43.2.1.

(A)~~a.~~ After the certified equipment has been returned to the county clerk by the applicable jurisdiction, and prior to use of the equipment in any primary, general, congressional vacancy, statewide ballot issue (including recall), or special election conducted by the county clerk, reinstatement or verification of the trusted build, ~~pursuant to~~ IN ACCORDANCE WITH Rule ~~43.8.11.3(a)~~ 43.2.11(B)(1), shall be completed.

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

(1)~~I.~~ Deliver the certified equipment to the jurisdiction;

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

(3)~~III.~~ Place one or more secure and numbered seals on the voting equipment ~~pursuant to~~ IN ACCORDANCE WITH Rule ~~43.8.2~~ 43.2.2. If during the

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

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

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

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

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

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

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

43.~~11~~5.3 Upon return of the certified voting equipment to the county clerk and recorder, the county clerk ~~shall~~ IS ~~not be~~ required to verify the trusted build if the documentation and chain of custody DOES NOT support the proper maintenance of the trusted build 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.

   the procedure should be documented and approved by SOS.

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.

   procedures for doing so should be documented and approved by SOS.

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.

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.