



June 6, 2014

Mr. Scott Gessler
Secretary of State
State of Colorado
Department of State
1700 Broadway, Suite 200
Denver, CO 80290

RE: Proposed Rules Concerning Voting System Conditions for Use, May 29, 2014

Dear Secretary Gessler:

Hart InterCivic is pleased to submit the attached document to the Colorado Department of State with our comments concerning the latest proposed rules about voting system conditions for use. We appreciate the main goal of developing a single set of clear and concise administrative rules and eliminating redundancy whenever possible.

We have reviewed the proposed rules carefully, and we do have some concerns and comments which we hope will be valuable to the Department of State. We appreciate your careful consideration of our input. (Our comments are noted inline, using the Adobe PDF comment feature). They appear in the following locations:

P. 1, Line 15	P. 3, Line 12	P. 6, Line 19
P. 2, Line 9	P. 3, Line 15	P. 6, Line 31
P. 2, Line 13	P. 6, Line 1	P. 7, Line 4
P. 3, Line 10	P. 6, Line 12	

Again, thank you for this opportunity to collaborate on the important task of continuously improving the rules concerning the use of election technology in the State of Colorado.

Sincerely,

A handwritten signature in black ink, appearing to read 'Edward P. Perez'.

Edward P. Perez
Director of Product Management
Hart InterCivic
Austin, Texas

Reference Copy – Hart InterCivic Comments to Proposed Rules Concerning Voting System Conditions for Use, May 29, 2014

For the full context in which the following comments are offered, please see the inline comments in the attached Adobe PDF. Comments are identified in the PDF by yellow “bubbles” at the pages and lines noted.

P. 1, Line 15

Hart InterCivic recommends that the language be amended to read, "*The County must provide each **accessible** DRE voter a headset with an adjustable volume control.*" In Hart Voting System v. 6.2.1, not all DREs are equipped with the module for accessibility, and the rules should specify that it is intended to apply only to those DREs so equipped with accessibility features.

P. 2, Line 9

Hart InterCivic recommends adding clarifying language that specifies that these rules are intended to apply to desktop PC workstations on which voting system application software is installed.

P. 2, Line 13

Hart InterCivic recommends adding clarifying language that this rule is intended to apply to **system**-level hardware passwords that are **not election-specific**, and that are **not** part of the election-specific device passwords that may be included in election definitions that are programmed by a third party vendor. For additional context, see our comments to 20.5.2 sub-section (e), below, on page 3, lines 10 and 12.

P. 3, Line 10

Hart InterCivic recommends adding the word "*county's*," before "*election management system*," so that the sentence reads, "*The voting system provider may not have administrative or user access to the **county's** election management system...*"

Hart InterCivic strongly recommends deleting the words "*or election database*," as access to the database is required in order for the vendor to program elections for smaller counties that do not own, and do not wish to own, ballot programming software. If the words "*or election database*" words are not deleted, it would effectively foreclose Hart's ability to provide ballot programming services for Colorado counties, thereby creating a great fiscal and resource burden on the counties, as they would be required to purchase their own ballot programming software (BOSS). Hart currently provides ballot programming services to 33 counties in Colorado. This would be an enormous change to their budget, workflow, and general election administration practices.

Furthermore, the new proposed language in 20.5.2 sub-section (e) does not appear to align with the intent of the language in the original use conditions, as the original language in the use conditions appears to be more concerned with protecting access to *desktop PCs*, while restrictions on the hardware voting devices are adequately covered in other parts of the use conditions.

P. 3, Line 12

Hart InterCivic strongly recommends deleting the words "*and device level passwords,*" as Colorado counties who use Hart's ballot programming service do not have the ability to change election-specific device-level passwords once their election has been programmed and their memory cards have been delivered. If these words are not deleted, it would effectively foreclose Hart's ability to provide ballot programming services for Colorado counties, thereby creating a great fiscal and resource burden on the counties, as they would be required to purchase their own ballot programming software (BOSS) and program their own ballots. Hart currently provides ballot programming services to 33 counties in Colorado. This would be an enormous change to their budget, workflow, and general election administration practices.

Furthermore, the new proposed language does not appear to align with the intent of the language in the original use conditions, as the original language in the use conditions appears to be more concerned with protecting access to desktop PCs, while restrictions on the hardware voting devices are adequately covered in other parts of the use conditions.

P. 3, Line 15

The intent of this rule is not clear to Hart, as it involves two different topics: prohibitions against connection to the Internet, and prohibitions against the use of Wi-Fi; those are not the same things. For example, 20.5.2 sub-section (g) below appears to allow the connection of voting system components via modem...does that include the possibility of using a broadband modem that functions over wireless public networks? Such connections could be accommodated by 20.5.2 sub-section (g), standing on its own, but 20.5.2 sub-section (f) would contradict that.

If the intent is to prohibit connection to the internet only, then we recommend striking the language prohibiting Wi-Fi connectivity, as that may contradict desired functionality that is permissible under sub-section G.

If the intent is to prohibit **any** kind of wireless communications, then the language should simply refer to "*wireless communications*" in a sub-section separate from prohibitions against connecting to the Internet. Again, those are two separate issues.

P. 6, Line 1

Hart InterCivic recommends adding clarifying language stating the final authoritative backup copy on a write-once CD need not be generated directly from the Election Management workstation PC, as it is possible that not all EMS workstations are so equipped with a CD-writing component (or with the ability to write CDs, even if the component is installed). In other words, the language should clarify that "*The County must export a backup copy of the election setup records immediately after downloading the final removable card or cartridge, and for retention purposes, the exported data must be stored on a read-only, write-once CD.*" Such language would permit the usage of a different workstation to actually create the backup CD, if necessary.

P. 6, Line 12

Hart InterCivic recommends deleting the word "Pause," as voting systems certified to federal standards prior to 2005 might not have the functional capability to "pause," strictly speaking. On the Hart Voting System that is currently certified in Colorado, users can prevent further advancement on an audio ballot by not turning the SELECT wheel on the eSlate DRE, but that that is not a "pause," strictly speaking.

P. 6, Line 19

Unless the Department of State specifically intends to require counties to purchase true UPS devices (which can be quite heavy and costly), Hart InterCivic questions whether "*uninterruptible power supply*" is the preferred wording. Are backup battery supplies that are sufficient to sustain continuous operation for a minimum of two hours acceptable, for example? Or does the Dept. of State want to actually require corded UPS devices that must be plugged into an outlet on the wall? UPS devices would create additional burdens in terms of cost, storage space in the warehouse, wall outlets required, and the total weight of equipment deployed to a voter service center.

P. 6, Line 31

Unless the Department of State specifically intends to require counties to purchase true UPS devices (which can be quite heavy and costly), Hart InterCivic questions whether "*uninterruptible power supply*" is the preferred wording. Are backup battery supplies that are sufficient to sustain continuous operation for a minimum of two hours acceptable, for example? Or does the Dept. of State want to actually require corded UPS devices that must be plugged into an outlet on the wall? UPS devices would create additional burdens in terms of cost, storage space in the warehouse, wall outlets required, and the total weight of equipment deployed to a voter service center.

P. 7, Line 4

The intent of this rule and the term "*override key*" is not clear to Hart. Is the intent of the rule to require polling official assistance for a voter that wishes to cast a ballot that has been rejected by the scanner? For example, if a voter over-votes a ballot, and the scanner rejects the ballot as mismarked, is the intent of the rule to require that the voter does not have the ability to override the rejection and cast the ballot without further assistance? If so, then Hart InterCivic recommends the use of more generic language that is less likely to have the unintended effect of requiring a very specific hardware implementation.

If our understanding of the intent of the rule is correct, then you might include language such as, "*The county must program each optical scanner in a manner such that voters who wish to override ballot rejections and cast rejected ballots 'as-is' shall be required to have the assistance of a polling official to execute the override.*"

If such clarifying language is not substituted, the proposed rule could be read as requiring optical scanner machines to override ballot rejections only through the use of a separate physical key (which is hopefully not the intention, because certainly not all machines are designed in such a manner).

Working Draft of Proposed Rules

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

May 29, 2014

Disclaimer:

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

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

Please note the following formatting key:

Font effect	Meaning
Sentence case	Retained/modified current rule language
SMALL CAPS	New language
Strikethrough	Deletions
<i>Italic blue font text</i>	Annotations


1 *Amendments to Rule 20.1:*

2 20.1 The county ~~clerk~~ must submit its annual security plan on the form prescribed by the
3 Secretary of State in accordance with section 1-5-616(5), C.R.S.

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

5 20.2.2 The county must maintain and document ~~the~~ UNINTERRUPTED chain-of-custody for
6 each voting device FROM THE INSTALLATION OF TRUSTED BUILD TO THE PRESENT,
7 throughout the county's ownership or leasing of the device. FOR VOTING SYSTEMS
8 ACQUIRED BEFORE MAY 28, 2004, THE COUNTY MUST MAINTAIN AND DOCUMENT
9 UNINTERRUPTED CHAIN-OF-CUSTODY FOR EACH VOTING DEVICE FROM THE
10 SUCCESSFUL COMPLETION OF ACCEPTANCE TESTING CONDUCTED ACCORDING TO
11 RULE 20.8.4.

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

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


1 *Amendments to Rule 20.4.1:*


2 20.4 Individuals with access to keys, door codes, and vault combinations-

3 20.4.1 For employees with access to areas addressed in Rule 20.4.3, the county must state
4 in the security plan each employee's title and the date of the ~~the~~ criminal
5 background check. [Section 24-72-305.6, C.R.S.]

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

7 20.5.2 In addition to the access controls discussed in Rule 20.4, the county must change
8 all passwords and limit access to the following areas:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

38 20.8.4 Upon completion of any maintenance, the county must verify or reinstate the trusted
39 build and conduct a full acceptance test of equipment that must, at a minimum,

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

6 20.8.5 The Secretary of State will annually inspect county maintenance AND CHAIN-OF-
7 CUSTODY records and verify THE INTEGRITY OF trusted build ~~installation~~ on a
8 randomly selected basis.

9 *Rule 20.9.3(d) formatting correction:*

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

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

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

17 *Amendments to Rule 20.11.2:*

18 20.11.2 Anonymity. The designated election official must implement measures to
19 protect the anonymity of voters choosing to vote on DREs.

- 20 (a) Measures to protect anonymity include:
- 21 (1) The county may not keep any record indicating the order in which
22 people voted on the DRE, or which VVPAT record is associated
23 with the voter.
 - 24 (2) When more than one DRE is available at a voting location, the
25 COUNTY MUST, TO THE EXTENT PRACTICABLE, ALLOW THE voter ~~must~~
26 ~~be given the choice as to which~~ TO CHOOSE THE DRE they would
27 ~~like~~ HE OR SHE WISHES to vote on, ~~to the extent practicable~~.

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

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

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

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

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

11 *New Rule 201.71:*

12 20.17 VOTING SYSTEM CONDITIONS FOR USE

13 20.17.1 THE COUNTY MUST USE THE VOTING SYSTEM ONLY ON A CLOSED NETWORK
14 AS DEFINED IN RULE 21.1.6 OR IN A STANDALONE FASHION.

15 20.17.2 THE COUNTY MUST USE ITS ELECTION MANAGEMENT SYSTEM AS DEFINED IN
16 RULE 21.1.9 OR OTHER EXTERNAL SOLUTION FOR THE ABSTRACT OF VOTES CAST
17 SENT TO THE SECRETARY OF STATE UNDER SECTION 1-10-103(1), C.R.S.

18 20.17.3 ACCESS LOGS.

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

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

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

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

1 20.17.4 THE COUNTY MUST CREATE A BACKUP COPY OF THE ELECTION SETUP
2 RECORDS ON A READ-ONLY, WRITE-ONCE CD, IMMEDIATELY AFTER DOWNLOADING
3 THE FINAL REMOVABLE CARD OR CARTRIDGE.

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

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

9 20.17.5 DREs.

10 (A) THE COUNTY'S ELECTION JUDGES MUST:

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

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

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

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

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

24 20.17.6 OPTICAL SCANNERS AS DEFINED IN RULE 21.1.13:

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

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

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

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

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

5 20.18 ES&S VOTING SYSTEM CONDITIONS

6 20.18.1 IF THE COUNTY MUST PROVIDE LANGUAGE MINORITY ASSISTANCE UNDER
7 SECTION 203 OF THE VOTING RIGHTS ACT (42 U.S.C. §§ 1973 to 1973bb-1), IT MAY
8 NOT USE AN ES&S VOTING SYSTEM.

9 20.18.2 DREs. THE COUNTY MAY ONLY USE THE NINE INCH SCREEN ON THE VVPAT.

10 20.18.3 FOR OPTICAL SCANNERS WITH A ZIP DISK DRIVE, THE COUNTY MUST SAVE THE
11 CAST VOTE RECORDS FOR EACH BATCH OF TABULATED BALLOTS TO A ZIP DISK
12 BEFORE SCANNING THE NEXT BATCH.

13 20.19 HART DRE CONDITIONS. IF A COUNTY SHORTENS A LENGTHY CANDIDATE NAME ON THE
14 VVPAT, IT MUST PROVIDE PRINTED NOTICE OF THE CHANGE TO VOTERS AT THE VOTER
15 SERVICE AND POLLING CENTER.

16 20.20 SEQUOIA DRE CONDITIONS

17 20.20.1 THE COUNTY MUST ADD CLARIFYING TEXT TO THE DISPLAY SCREEN DURING
18 THE VVPAT REVIEW PROCESS THAT INSTRUCTS THE VOTER TO REVIEW HIS OR HER
19 BALLOT CHOICES.

20 20.20.2 THE COUNTY MUST LOCK THE ACTIVATE BUTTON TO PREVENT ITS USE
21 DURING AN ELECTION.

22 20.20.3 A COUNTY MAY NOT MODIFY THE SCREEN DISPLAY USING AN OVERRIDE.INI
23 FILE WITHOUT APPROVAL FROM THE SECRETARY OF STATE.