7-29-13 Commission Packet Contents:

1. Meeting agenda
2. Comments from Harvie Branscomb
3. Original RFQ for assessment of voting systems technology
4. SLI response to RFQ
5. June 11 memo from UVS Advisory Committee to Secretary Gessler re: UVS RFP
6. July 18 memo from UVS Advisory Committee to Secretary Gessler re: delay of UVS RFP to October 1.
7. Security notes: Commissioner Matsumoto’s markup
9. Rules recodification matrix
10. Proposed new election rules
Notice of Meeting

Colorado Voter Access and Modernized Elections Commission

Date of Notice: July 23, 2013
Date and Time of Meeting: July 29, 2013, 1:00 p.m.

I. Notice of Colorado Voter Access and Modernized Elections Commission meeting
You are hereby notified that the Colorado Voter Access and Modernized Elections Commission will meet to discuss the items listed below.

The meeting is scheduled for July 29, 2013, at 1:00 p.m. in the Aspen Conference Room, located on the third floor of the Secretary of State’s office at 1700 Broadway, Denver, Colorado 80290.

II. Invitation for public comment
All meetings of the Colorado Voter Access and Modernized Elections Commission are open to the public. To submit comments in writing, please call (303) 894-2200 x6318 for email instructions.

III. Meeting agenda
- Open public comment (Please limit comments to three minutes or less)
- SLI Global Solutions - discuss second needs assessment
  Note: UVS Advisory Committee Chair Debra Johnson and UVS Public Participation Panel Chair Clarissa Thomas will be present for this discussion at the Commission’s request.
- Business Practices Subgroup briefing
- Security discussion
- NCOA Update

IV. Meeting materials
All documents and materials for the Commission meeting are available to the public online. To view or download these materials, visit the Colorado Voter Access and Modernized Elections Commission page on the Secretary of State’s website.

V. Broadcast and audio recording of the meeting
To access audio broadcasts of the Voter Access and Modernized Elections Commission meeting, visit the Audio Broadcasts page on the Secretary of State’s website.

VI. Office contact
If you have any questions or concerns, please contact our office at (303) 894-2200 ext. 6318.
Steven, Andrew
Thanks for putting me on the list for notice of the COVAMEC meetings. I have learned that the COVAMEC meetings are the best and perhaps the only means to learn what is happening with Colorado elections, for the time being. I am even learning about facts about the public body that I serve on, the CO UVS PPP.

I have attached a list of questions that I think the COVAMEC should be prepared to answer in preparation of its September report on voting systems technology. The questions are posed to learn how the existing technology is used, and how it would be expected to be used under 1303 changes.

I believe that the Dept. of State should be prepared to answer these questions and I hope that the COVAMEC will ask CDOS to do so. A voting system is not just the hardware that is provided- it is the procedures that are used with it- and these do vary around the state.

Harvie Branscomb

The following are specific questions about the November elections in 2011 and 2012 and then about the November 2013 upcoming election (answers that are within 5% accuracy are sufficient- exact answers are not necessary):

In the 2011 November election:
(simply circle the bold face letter signifying the answer or fill in the number asked for)

Did you use election-day precinct or vote-center polling or mail-ballot model? e/ v /m How many voted/cast ballots printed by Ballot on Demand?

How many voted/cast paper ballots total? Using e-pollbooks or paper pollbooks? e / p Explain any local variation on the use of pollbooks in following lines e.g. cards instead of books...?

How many election judges? Do county staff serve as election judges?
y / n How many judges are year-round employees of the county?

How many certified watchers? How many canvass board members not including the clerk? Is the clerk or other election staff on the canvass board? y / n

How many central count scanners used? Scanner model #s Hand counting for unofficial and official count? y / n
In the 2012 November general election:
Vote-center model for election day? y / n Using e-pollbooks or paper pollbooks? e / p Explain any local variation on the following lines e.g.
cards instead of books...?

How many ballots printed by Ballot on Demand? ____ Approximately how BOD ballots many left unused? ____ How many total voted/cast paper ballots? ____

(For the next few questions - circle a for "all major classes of ballots", m for "a majority of ballots", s for "some ballots", n for "none at all" -- circle each that applies)

Ballots printed by election vendor? a / m / s / n Ballots printed by print shop? a / m / s / n Ballots printed in county? a / m / s / n
Ballots printed by county election staff? a / m / s / n By election judges? a / m / s / n

Stubs on ballots? a / m / s / n Stubs printed independently of the face content of the ballot? y / n

Ballots folded/ inserted by election vendor (printer, mailing house, etc)? a / m / s / n Ballots folded/inserted by county staff? a / m / s / n
By election judges? a / m / s / n

Ballot envelopes addressed by election vendor? a / m / s / n Envelopes addressed by other contractor? a / m / s / n Envelopes addressed by county election staff? a / m / s / n By election judges? a / m / s / n

Envelopes delivered to USPS by election vendor? a / m / s / n Envelopes delivered by other contractor? a / m / s / n Envelopes mailed by county election staff? a / m / s / n By election judges? a / m / s / n Bulk mail permit? a / m / s / n

Replacement ballots/envelopes provided by election staff? y / n Replacement ballots/envelopes provided by election judges who are not staff? y / n.

Envelope sorters in use for returned mail-in? y / n Used to sort by precinct/ballot style? y / n Automated detection of identity of returned envelope (not manual bar code reading)? y / n Manually scanned bar code transmitted to SCORE? y / n Manual entry of returned envelope identity to SCORE? y / n

How many ballot envelopes returned? ____ How many envelopes rejected for signature discrepancy? ____ How many envelopes rejected for missing ID? ____ How many other envelopes rejected before 7PM ED? ____ Automated signature verification in use? y / n How many signatures on physical
envelopes were viewed directly by human eyes? ___ How many signatures on envelopes viewed as digital images? ___ Result of human signature verification automatically transmitted to SCORE? (r for in real-time, b for batched electronic transfer, m for manual entry into SCORE)? r / b / m. Approx. how many hours delay maximum between signature verification decision and entry in SCORE? 

Approx. how many full time staff involved in signature verification? ___
Approx. how many election judges involved in signature verification? ___
Approx. how many man hours used for signature verification? ___ How many people work together to verify a signature? 1 / 2 / 3 / more

How many election judges? ___ Do county staff perform functions of election judges? y / n How many judges are year-round employees of the county? ___

How many certified watchers? ___ How many canvass board members? ___

Approx. how many man hours used for audit? ___ About how many people involved in conducting audit? ___ How many days used for audit? ___ Date of first day of audit? _______ Date of last day of audit? _______ How many ballots manually counted for audit? _______

Did you move uncounted election day precinct polling ballots to a central location for counting? y / n Were some ballots moved before the polls were closed? y / n Were the polling-place election judges responsible to count the number of ballots before sending the ballots to central counting? y / n Do you use security sleeves for transfer of ballots to ballot box or scanner? y / n

How many central count scanners used? ___ Model #s of scanners ________________

Date of earliest opening of mail ballot envelope? _______ Date of first scanning of mail-in ballots? ______ # of days on which mail ballot scanning took place? ______

# of full time staff (not election judges) involved in central count? ___ # of election judges (not staff) involved in central count? ___ # of full time staff who are election judges involved in central count? ___

Approx. # man hours used for central count? ___ # of central count locations (separate buildings)? ___ # of rooms used for central count? ___
How many early voting centers? __

Concerning early voting locations - not clerk's offices (2012 General):

How many clerks offices? ____
How many early voting locations outside of clerk's offices? _____
How many early voting locations provided replacement mail-in ballots/envelopes? ___

Flat ballots provided at early voting centers outside of clerks offices (no identifiable envelope)? y / n Flat ballots provided at early voting centers inside of clerks offices (no identifiable envelope)? y / n Voter places ballot in scanner at early voting? y / n How many DRE votes from early voting? __ How many flat paper ballots cast at early voting? ____ How many replacement mail-in ballots/envelopes provided? __ How many ballots/envelopes turned in for replacement? ____ How many DRE used for early voting (total)? ____ How many optical scanners used for early voting (don't include central count scanners if at another location)? ____

Approx. farthest distance from a voter to an early voting location by road? ____ Approx. farthest distance from a voter to their assigned polling place? ___

Planning for the 2013 election:

Approx. how many voters expected? ____ How many polling centers would be required? ____ How many polling centers are anticipated to be deployed? ____

Do you plan to provide flat ballot voting and anonymous casting of ballots (no identifiable envelopes) into ballot boxes at all polling centers? y / n ...at some polling centers y / n

Do you plan to provide voter-visible counting of flat ballots at all polling centers? y / n at some polling centers? y / n

Will you check eligibility (statutory ID-check) at polling centers for casting of flat ballots? y / n

Is there a possibility of an eligibility check (statutory ID-check) at polling centers for return of unsigned mail-in ballot envelopes that will not require subsequent signature verification? y / n

Do you plan to use a voter accessible electronic pollbook for check-in? y / n

Method of polling center voter check-in (x all that apply) ( )mail-ballot application ( )other form ( )voter operated e-pollbook ( )election-judge using SCORE ( ) staff using SCORE ( ) signature card; ( )other ________________________________
Workers at polling centers will be ( ) election staff ( ) election judges ( ) both

Will you use BOD to print ballots? ( )none ( )emergency-and-last-minute ( )some-but-not-all ( )all

Will you print stubs on ballots? (all; majority, minority, none) a / m / s / n Will you detach the stubs from mail-in ballots before removing the ballots from their secrecy sleeves? y / n

Will you check the stub or ballot style of incoming mail-in ballots to confirm the ballot style is correct for the voter? y / n What is your anticipated farthest distance from an elector’s residence to a polling center? _____

[Please add and answer other questions that ought to be asked here...]

----- end of list of questions regarding 2011, 2012, 2013 elections -----
Request for Quotes
Assessment of Voting Systems Technology

Background

In 2013, the Colorado General Assembly passed HB 13-1303, which, among other things, establishes the Colorado Voter Access and Modernized Election Commission. Under section 1-1-115(6)(b), C.R.S., the Commission must prepare and present an independent needs assessment that assesses the current state of technology, including voting systems, certification of voting systems, and replacement of voting systems. The report must also include an analysis of election-related technological costs and funding sources. The Commission must present the needs assessment to the State Affairs committees of the House of Representatives and the Senate by September 2, 2013. (Please see the attached bill summary for a comprehensive summary of HB 13-1303.)

Purpose

The purpose of this request is to obtain documented quotes from vendors who can assist the Colorado Department of State (DOS) and the Commission with preparing the needs assessment. The DOS will consider each response to this request as a formal quote and will evaluate them with the intent of awarding the project to the successful respondent.* Submitted quotes should include sufficient information to address the requirements outlined in this request, but should not include confidential information; responses are considered public information and will be handled as such by the DOS.

*Respondents are responsible for all expenses associated with responding to this request. The DOS will not pay for any information or ideas submitted in response to this request or for any costs incurred by any party as a result.

Documented Quote Requirements

The respondent’s quote must fully address each of the requirements listed below. In preparing the quote, respondents should consider all activities necessary to meet requirements and the associated costs for each.

1. **Scope of project.** The selected vendor must meet with key DOS and county staff on the scope of this project and prepare a Statement of Work that includes activities, timelines, and deliverables. Under the direction of the DOS and in consultation with the Commission, the needs assessment must describe:

   A. The current state of technology relating to:

   1. Voting Systems. This must include an analysis of voting systems currently used in Colorado and voting systems that may be available that allow counties to conduct elections in accordance with the provisions of HB 13-1303 and the Colorado election code.

   2. Certification of Voting Systems. This must include an analysis of voting systems currently certified for use in Colorado, the availability of voting systems that are certified by the U.S. Election Assistance Commission (EAC) but not yet certified in Colorado, and the process and timeline for certifying voting systems that are not
currently certified by Colorado, the EAC or any other State.

3. Replacement of Voting Systems. This must include an analysis of counties’ needs for replacing voting systems, the types of systems necessary under the new election model, as well as timing issues based on the elections calendar. This analysis must also consider the implications of the DOS initiative to develop a uniform voting system throughout the state.

B. The election-related technological costs and funding sources, including:

1. An estimate of necessary equipment costs to conduct elections as described in HB 13-1303 and the Colorado election code.

2. An analysis of funding sources that are or may will be available for the purchase of new voting systems.

In addition, the vendor must draft and provide the report to the Commission for presentation to the General Assembly.

2. Reports. Vendor must provide weekly written reports to the DOS and oral reports to the DOS and the Commission as requested.

**Documented Quote Responses**

The response must be comprehensive and must include any travel estimates. The DOS will not provide office space or equipment. The quote must not exceed $24,000.

The response must include a brief company overview describing the company’s experience, qualifications, and expertise relevant to the requirements, as well as any staffing considerations and unique qualifications for this project (e.g., past successes with similar projects and government entities) and disclosure of any potential conflicts of interest.

The response will be evaluated based on:

1. The overview of the company’s experience, qualifications, and expertise in creating needs assessments reports;

2. Specific experience analyzing drawbacks and benefits of implementing standard technology and procedures in a widely-varying, multi-jurisdictional environment;

3. Specific experience in creating effective change-management plans in a multi-jurisdictional public sector environment; and

4. The activity plan and cost estimate contained in the response.

Preference may be given to companies with referenced experience in the area of elections and voter registration.
How to Respond

Any vendor interest in submitting a documented quote in response to this request should make such submission to the DOS no later than the close of business, 3:00 p.m., MDT, on Wednesday, July 17, 2013. Responses received after the deadline will not be considered. Responses may be delivered via person, mail, fax, or email to:

Ryan Moyle
Department of State
1700 Broadway Suite 200
Denver, CO 80290
Fax: 303-869-4860
Email: ryan.moyle@sos.state.co.us

Questions regarding this request should be submitted to Ms. Lizotte via email only.

Contract and Compensation

The Department of State will evaluate all responses as soon as possible. The Department will issue a purchase order to the selected vendor. A copy of the State of Colorado purchase order terms and conditions is available at http://www.colorado.gov/dpa/dfp/sco/contracts/fiscalrules/PO_Terms_&_Conditions_1-1-09.pdf. Before beginning work for this project, the vendor must be registered with the Department of State and be in good standing to do business in the State of Colorado.
House Bill 13-1303 implements various changes to the "Uniform Election Code of 1992" (code).

Residency. Currently, to be eligible to register to vote, a person must have resided both in the state and in the precinct in which he or she intends to register for at least 30 days prior to an election. The bill shortens the time required for state residency to 22 days and eliminates the minimum time that an elector must have resided within a Colorado precinct.

Registration. Under current law, voter registration must be effected no later than 29 days before an election for a person to cast a ballot in that election. The bill expands the time during which a person may register to vote in an election, and describes the deadlines associated with the various methods of voter registration. Specifically, a person may register by:

- Submitting a voter registration application through the mail, a voter registration agency, or a voter registration drive no later than 22 days prior to an election;

- Appearing in person at his or her county clerk and recorder's office when registration is permitted at the office or submitting an application at a high school in accordance with high school registration procedures;

- Applying via a local driver's license examination facility or through the on-line voter registration system maintained by the secretary of state through 8 days prior to an election;

- Visiting a voter service and polling center during the time that such location is open, including on or prior to the date of the election.

The bill harmonizes the content of self-affirmations made in connection with registering to vote.

Mail ballot elections. Under the bill, a mail ballot election is an election for which active registered electors receive a ballot by mail and may then cast the ballot by mail, deposit it at a drop-off location, or go to a voter service and polling center to cast a ballot in person. The bill requires all general, primary, odd-year, coordinated, presidential, special legislative, recall, and congressional vacancy elections to be conducted as mail ballot elections. Consequently, the ability of an elector to apply for permanent mail-in status is removed from the code. The bill limits current code provisions relating to early and mail-in voting to municipality and special district elections conducted under state law.
Voter service and polling centers and ballot drop-off locations. To complement the implementation of mail ballot elections, the bill requires county clerk and recorders to establish a minimum number of voter service and polling centers, depending on the number of active registered voters in the county. Factors that county clerk and recorders must consider in designating voter service and polling centers are enumerated.

Each voter service and polling center must provide the following:

- The ability for an eligible elector to register to vote;
- The ability for an eligible elector to cast a ballot;
- The ability for an eligible elector to update his or her address;
- The ability for an eligible elector who has legally changed his or her name to have his or her name changed in the registration records;
- The ability for an unaffiliated registered elector to affiliate with a political party and cast a ballot in a primary election;
- Secure computer access; except that smaller counties may seek a waiver of this requirement upon demonstrating hardship and securing approval of a plan to access the statewide voter database and conduct real-time verification of voter eligibility via telephone or other means;
- Facilities and equipment for persons with disabilities, including direct record electronic voting machines or other voting systems accessible to electors with disabilities;
- Voting booths;
- Original and replacement ballots for distribution;
- Mail ballots to requesting electors;
- The ability to accept mail ballots that are deposited by electors; and
- The ability of a person to cast a provisional ballot.

In addition to voter service and polling centers, certain counties must also establish stand-alone drop-off locations.
Inactivity by reason of failure to vote. The bill repeals the category of voter inactivity that is triggered by an elector's failure to vote and makes all such voters active. As a result, such voters will receive mail ballots in future elections.

Electronic communications transmission. Except for ballots and voter information cards, upon request, county clerks and recorders are authorized to transmit electronically elections-related communications to voters.

Colorado voter access and modernized elections commission. The Colorado voter access and modernized elections commission (commission) is created for the purpose of evaluating implementation of the bill and assessing systems used in the state for voting and registration. The composition, terms, and duties of the commission are specified, and the commission is directed to prepare and present 4 separate reports to the state, veterans, and military affairs committees of the house of representatives and the senate. The commission is subject to the sunset review process for newly created advisory committees.

Accuracy of voter information. Beginning July 1, 2013, the secretary of state must conduct a monthly national change of address search on all electors whose names appear in the statewide voter registration list. The secretary of state must transmit data gathered in such searches to county clerk and recorders, who are required to update electors' records pursuant to statutorily prescribed procedures.

Currently, the secretary of state and the department of revenue maintain a reciprocal information-sharing agreement that allows each entity to verify information provided in connection with applications for voter registration. The bill directs the secretary of state to enter into similar information accessibility agreements with the department of public health and environment and the department of corrections.

Terminology. The bill alters various terms used in the code, including:

- Replaces "voter information card" with "confirmation card";
- Except in the case of municipal and special district elections, replaces "polling place" with "voter service and polling center", and creates the term "polling location" to refer to voter service and polling centers or polling places, as applicable;
- Changes the term used to describe overseeing election judges from "supply judge" to "supervisor judge"; and
- Implements "people first" drafting where applicable.
Proposal To:
State of Colorado
Department of State (DOS)

For:
RFQ # DQ2-1303-SCORE
Assessment of Voting System Technology
July 17, 2013

Mr. Ryan Moyle
State of Colorado
Department of Personnel/General Support Services
Denver, CO 80203

RE: RFQ – DQ2-1303-SCORE, Assessment of Voting System Technology

Mr. Moyle:

The State of Colorado Department of State (DOS) and the Colorado Voter Access and Modernized Election Commission must assess our State’s current election systems technology, including counties’ voting systems, certification of voting systems, and the need for upgrading, enhancing or replacing these systems. This assessment will allow the state to have access to current and accurate information about voting products currently deployed, the technology needs of counties to conform to HB 13-1303 and related statutory requirements, and the availability of new voting product solutions and associated costs that meet those needs.

As an EAC-accredited VSTL headquartered in Denver, CO, SLI has the extensive voting system knowledge and proven assessment methodologies that are needed to assist DOS and the Commission with preparing the needs assessment. SLI recognizes the challenge of the timeframe to complete this effort to support the informational needs of the House and Senate affairs committees by September 2, 2013. We have constructed our proposal with this in mind based on our unique expertise in as an accredited EAC Voting System Test Lab (VSTL), as well as our experience with dozens of government agencies providing independent assessment services.

As a Colorado-based company with national reach, we are confident that the SLI solution will fulfill your needs in a cost competitive manner, while helping to ensure results that meet the business needs of the State of Colorado and the citizens it serves.

SLI Global Solutions acknowledges and accepts all term and conditions of this RFQ.

SLI Global Solutions, Inc. is a privately-held Colorado corporation with our office location at:

216 16th Street, Suite 700
Denver, CO 80202
SLI’s Point of Contact for this proposal is:

Traci Mapps, Senior Director of Operations – Compliance Division
216 16th Street, Suite 700
Denver, CO 80202
720-975-9199 office
480/620-5907 cell
tmapps@sliglobalsolutions.com

I, Traci Mapps, as Senior Director of Operations – Compliance Division of SLI Global Solutions (SLI), am authorized to sign this proposal and bind our company to it and any ensuing contract. As well as, serve as the principal point of contact between SLI and Colorado Department of State (DOS) with respect to all operational issues relating to the services and/or deliverables.

We look forward to your review of our proposal.

Sincerely,

Traci Mapps
Senior Director of Operations – Compliance Division
ASSESSMENT OF VOTING SYSTEMS TECHNOLOGY

The purpose of this request is to obtain documented quotes from vendors who can assist the Colorado Department of State (DOS) and the Commission with preparing the needs assessment. The DOS will consider each response to this request as a formal quote and will evaluate them with the intent of awarding the project to the successful respondent.* Submitted quotes should include sufficient information to address the requirements outlined in this request, but should not include confidential information; responses are considered public information and will be handled as such by the DOS.

The report must also include an analysis of election-related technological costs and funding sources. The Commission must present the needs assessment to the State Affairs committees of the House of Representatives and the Senate by September 2, 2013. (Please see the attached bill summary for a comprehensive summary of HB 13-1303.)

The Colorado Voter Access and Modernization Election Committee must assess the current state of voting technology, the voting system certification process and options for enhancing, upgrading or replacing the systems in use today. By statute, a thorough needs assessment must be presented to the State Affairs committees of the Colorado House of Representatives and the Senate by September 2, 2013. The Colorado Department of State (DOS) and the Commission have requested quotes from qualified vendors to provide expert assistance in developing the analyses, assessments and reports needed to comply with this requirement.

SLI Global Solutions (SLI), based in Denver Colorado, has earned a national reputation for helping state election agencies and voting clients ensure projects are planned, executed, monitored, and controlled efficiently and effectively. SLI brings over 12 years of experience with voting system projects for state, federal and international clients. SLI offers DOS and the Commission local access to unparalleled experience and expertise to ensure a comprehensive needs assessment is developed to effectively guide future funding, technology and policy decisions. SLI offers:

- **A Voting System Test Lab (VSTL) with Direct and Relevant Voting Certification Test Experience.** SLI Global Solutions (SLI) has been an Independent Test Authority (ITA) since the National Association of State Election Directors (NASED) first established an ITA certification program in 2001. SLI is an accredited Voting System Test Lab (VSTL) by the National Institute of Standards and Technology (NIST) under the National Voluntary Laboratory Accreditation Program (NVLAP) – ISO 17025, and by the EAC. SLI has provided testing, source code review, independent assessment, IV&V, and security services on voting/election engagements with Secretary of State Offices and Election Boards including California, Florida, Minnesota, North Dakota, New Mexico, New York, Ohio, Oklahoma, and Pennsylvania. Our experience also includes international projects for the Republic of Philippines and helping to establish certification requirements for internet-based systems for uniformed and overseas voters. Colorado can count on SLI to provide detailed and comprehensive Voting System assessment services.

- **World-Class Methodologies.** SLI is an ISO 17025 accredited test lab and ISO 9001:2008 certified company in Quality Management. Our organization follows the principles espoused by the Project Management Institute (PMI) as embodied in its Project Management Body of Knowledge (PMBOK® Guide) and the International Council on Systems Engineering (INCOSE) Systems Engineering Handbook. SLI adheres to the team-driven, client-focused approach to project management, ensuring quality, cost and schedule performance.

Managing technology risk
Managing Body of Knowledge (PMBOK), IEEE, and CMMI Standards. Our process maturity gives you confidence that our efforts will be well managed and effectively executed.

- **Local Team with National Reach.** To assist DOS and the Commission with the assessment of voting equipment and certification, we are proposing Colorado-based staff that is experienced with multiple voting manufacturers in federal as well as state projects. Our team’s extensive credentials, and relevant experience and knowledge, ensures that DOS and the Commission will have access to the most qualified voting systems expertise in the industry. Additionally, since we are Colorado-based, we can effectively interact, meet and coordinate with DOS and Commission staff as required throughout the project.

### Section Organization

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SLI Voting Experience and Qualifications</td>
</tr>
<tr>
<td>2</td>
<td>Voting Assessment Process and Process</td>
</tr>
<tr>
<td>3</td>
<td>Voting Technology Assessment</td>
</tr>
<tr>
<td>4</td>
<td>Costs and Funding Sources</td>
</tr>
<tr>
<td>5</td>
<td>Cost Proposal</td>
</tr>
</tbody>
</table>

### 1. SLI Voting Experience and Qualifications

The overview of the company’s experience, qualifications, and expertise in creating needs assessments reports: Specific experience analyzing drawbacks and benefits of implementing standard technology and procedures in a widely-varying, multi-jurisdictional environment; Specific experience in creating effective change-management plans in a multi-jurisdictional public sector environment

SLI Global Solutions, Inc. (SLI) is an ISO 9001:2008 certified and ISO 17025 accredited company headquartered in Denver, with project locations in capital cities within the US and internationally. Since our founding in 1996, SLI’s focus has been on helping customers build quality and innovation into their products and system implementations, while minimizing technology risk. SLI provides the following services to both public and private sector clients worldwide:

- Independent Verification and Validation, including business and technical assessments
- Quality Management, including Quality Planning, Quality Assurance, Quality Control and Testing
- Outsourced Software Test Engineering, including Functional, Regression, System, Integration and Compatibility Software Testing (Load, Stress, Automation, and Performance Testing)
- Test Management for large systems development projects. This includes oversight and direction for vendor-led testing for a State client and development and execution of State-led testing
Managing technology risk


SLI has provided Voting System Testing and Certification services for over 12 years. Under the auspices of the National Voluntary Laboratory Accreditation (NVLAP) Program of the US National Institute of Standards and Technology (NIST), in partnership with the United States Election Assistance Commission (EAC), SLI is an accredited Voting System Test Laboratory (VSTL). Our VSTL is specifically accredited to laboratory standard ISO 17025. SLI has been there from the very onset of national testing standards for voting equipment and continues today as the premier provider of these services, including:

- Document Review
- Independent Assessments
- Source Code Review
- Functional Testing
- Security Testing
- Hardware Testing
- Election Night Reporting Stress / Performance Testing
- Pre- / Post-Election Verification Services
- Voting System Standards Development

SLI has extensive experience with all variations of voting systems, components, and configurations from the majority of top voting system manufacturers in the US and international markets. SLI has provided in-depth testing and technical analysis on:

- Election Management Systems
- Direct Record Electronic systems (DRE)
- Optical Scanners
- Ballot Marking Devices
- Central Count Scanners
- Ballot on Demand systems
- Internet Voting
- Voter Registration Systems

SLI and our employees have earned a variety of voting related certifications and accreditations in quality, testing, audit, and security. This information is detailed below in the Exhibit 1-1, *SLI Certification Profile*. 
# Recognition and Certification Profile

<table>
<thead>
<tr>
<th>Name of the Certification</th>
<th>Issuing Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Organization for Standardization (ISO) 9001:2008 Certified</td>
<td>SLI Global Solutions’ Quality Management System is applicable to: Quality and Risk Management Services, including Quality Assurance, Testing, and Independent Verification and Validation (IV&amp;V) for Software Applications and Computer Systems</td>
</tr>
<tr>
<td>United States Election Assistance Commission Certificate of Accreditation</td>
<td>Testing of voting systems under the EAC Voting System and Testing Program and Lab Accreditation. EAC Lab Code: 0701</td>
</tr>
<tr>
<td>United States Department of Commerce, National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP)</td>
<td>Accredited to certify voting hardware and software systems ISO/IEC 17025:2005 NVLAP Lab Code: 200733-0</td>
</tr>
<tr>
<td>International Organization for Standardization (ISO) ISO 19011 Leader Auditor, ISO 17025 Auditor, ISO 13485 Auditor, Internal 9001 Auditor</td>
<td>International Organization for Standardization (ISO) for Auditing</td>
</tr>
<tr>
<td>Accredited Test Lab (ONC-ATL)</td>
<td>United States Department Health and Human Services, The Office of the National Coordinator for Health Information Technology (ONC)</td>
</tr>
<tr>
<td>Project Management Professional (PMP) Project Management Institute (PMI)</td>
<td>Project management in accordance with PMBOK Standards and Processes</td>
</tr>
<tr>
<td>International Software Testing Qualifications Board (ISTQB) Certified Tester, Foundation Level (CTFL)</td>
<td></td>
</tr>
<tr>
<td>CISSP Certified Information Systems Security Professional (CISSP)</td>
<td>Independent certification governed by (ISC)^2(^3) the CISSP program earned ANSI ISO/IEC Standard 17024:2003 accreditation. Approved by the U.S. Department of Defense (DoD) in both Information Assurance Technical (IAT) and Managerial (IAM) categories.</td>
</tr>
<tr>
<td>(CRISC) Certified in Risk and Information Systems Control</td>
<td>ISACA is an independent, nonprofit, global association dedicated to assisting individuals and organization manage IT risk</td>
</tr>
</tbody>
</table>

Exhibit 1-1: SLI Certification Profile. SLI and its staff have earned a number of industry certifications to support the IV&V, QA, Testing, and Assessment work we perform for a wide variety of clients.

## 1.1 Relevant Voting Experience

SLI has extensive knowledge of the voting industry which includes practical application of standards and best practices, and an end-to-end understanding of the election process. SLI has the experience with Voting Systems and Voting manufactures that is needed to perform the work...
required by this RFQ. SLI’s portfolio of satisfied customers includes US state governments, the EAC, and international election bodies, and most major electronic voting system manufacturers around the globe. Our experience covers all evaluation criteria in your RFQ. The following table shows several examples of how our experience aligns with RFQ evaluation criteria. Following this table we provide a narrative summary of selected projects that are directly related to this RFQ.

<table>
<thead>
<tr>
<th>Project</th>
<th>Requirement Met</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wisconsin Voter Registration System (SVRS)</td>
<td>✓</td>
</tr>
<tr>
<td>Florida Voter Registration System IV&amp;V Services</td>
<td>✓</td>
</tr>
<tr>
<td>Pennsylvania Department of State QA Assessment of Election Readiness</td>
<td>✓</td>
</tr>
<tr>
<td>Specific experience analyzing drawbacks and benefits of implementing standard technology and procedures in a widely-varying, multi-jurisdictional environment</td>
<td></td>
</tr>
<tr>
<td>Iowa Eligibility (ELIAS) QA</td>
<td>✓</td>
</tr>
<tr>
<td>Pennsylvania Department of State QA Assessment of Election Readiness</td>
<td>✓</td>
</tr>
<tr>
<td>UOCAVA (Uniformed and Overseas Citizens Absentee Voting Act) Voting System Testing</td>
<td>✓</td>
</tr>
<tr>
<td>Specific experience in creating effective change-management plans in a multi-jurisdictional public sector environment</td>
<td></td>
</tr>
<tr>
<td>Alabama SACWIS QA and IV&amp;V</td>
<td>✓</td>
</tr>
<tr>
<td>Louisiana DCFS One Transformation QA</td>
<td>✓</td>
</tr>
<tr>
<td>Washington Provider Compensation System (PCS) QA</td>
<td>✓</td>
</tr>
<tr>
<td>Wisconsin Voter Registration System (SVRS)</td>
<td>✓</td>
</tr>
<tr>
<td>North Carolina MMIS + Program – Test Management Services</td>
<td>✓</td>
</tr>
</tbody>
</table>

Selected examples of our related experience in the Voting industry are summarized below:

**New York State Board of Elections (NYSBOE) Independent Assessment**

Client: New York State Board of Elections


SLI is contracted by the NYSBOE to act as the State’s federally certified Independent Testing Authority (ITA) for the purpose of examination and testing for the State Board’s certification, decertification, and re-certification of voting systems. SLI employed examination and testing
Managing technology risk

procedures, as required by the US Election Assistance Commission (EAC) program, plus the additional requirements specified by NYSBOE and required by New York State laws and regulations to test ES&S and Dominion systems submitted to NYSBOE for certification. Assessments include:

- All source code reviewed for compliance to the 2005 VVSG
- All source code had security review for NIST/FIPS compliance in the areas of encryption, back doors, SQL Injection, Trojans, Viruses, Worms
- All source code was hashed to assure no changes were made, then binaries were generated from this source code and place in a repository
- Thousands of pages of technical and training documentation were reviewed for accuracy and completeness
- All data transmitted and/or written to removable media was examined to assure that data was either encrypted and/or digitally signed
- Full functional and physical configuration audits were completed
- Voting system hardware was tested for compliance to standards

Since the initial certification of voting systems for the State of New York, SLI has continued to assist NYSBOE in testing modifications and enhancements to the Dominion and ES&S systems to ensure compliance with all requirements is maintained.

New Mexico Ballot on Demand Testing
Client: New Mexico Secretary of State
09/2011 – 01/2012

SLI performed testing on the multi-vendor and multi-jurisdiction ballot generation systems for adherence to Ballot on Demand Standards for New Mexico. The scope of work for this project was completed in seven (7) phases:

1. **Project Start Up**: Coordinated a kickoff meeting with the New Mexico Secretary of State and Runbeck Election Systems (Vendor) to clarify all tasks associated, discuss the timeline and to identify any potential obstacles.
2. **System Familiarization**: SLI underwent a familiarization of the various on demand ballot generation systems to gain a sufficient knowledge base of the systems under test.
3. **Documentation Review** Conducted a document review to evaluate the extent to which the Vendor’s on demand ballot generation system conforms to the hardware requirements identified in the Ballot on Demand Standards for New Mexico.
4. **Test Creation and Validation**: SLI created and validated test cases using the Ballot on Demand Standards for New Mexico. SLI applied our validated suite of voting system test methods to ensure that repeatability and transparency of results are attained in a cost-effective manner.
5. **Official Test Execution**: Performed certification testing to validate that the Vendor’s on demand ballot generation system operates as expected against the Ballot on Demand Standards for New Mexico.
6. **Administration and Reporting:** Prepared a final Test Report that outlined the testing performed for the Ballot on Demand Testing project and documented SLI’s findings based upon the reviews and tests executed.

7. **Project Close Out:** SLI returned equipment to the identified Vendor and archived test materials.

**Oklahoma Certification Voting System**
**Oklahoma Secretary of State and Hart InterCivic**
**8/2011 – 10/2011**

SLI conducted a certification assessment of Hart InterCivic’s voting system for the use in the State of Oklahoma. The certification process included document review, source code review, accuracy testing, security testing, functional testing and a hardware review to verify Hart’s voting system compliance with requirements given by the State. SLI’s task and deliverables included:

- **TDP and Hardware Delivery:** Received and conducted a Technical Data Package (TDP) Check-in of any/all delivered documentation and source code.
- **Documentation and Source Code Review:** Conducted a document review to evaluate the extent to which it conforms to the requirements. Performed validation of fixes provided by Hart on discrepancies reported. Documentation review was limited to a technical data package (TDP). Performed Source code review on systems updates.
- **Functional Configuration Audit and Readiness Test:** Performed Functional Configuration Audit of Hart test documentation and functional tests and conduct a sampling of the tests executed by Hart. SLI also repeated the agreed “Readiness Test” performed by Hart.
- **Hardware Review and Check-In:** Performed an Operational Status Check on incoming hardware to confirm the operational status of the equipment and ensure its preparedness for the Readiness Test.
- **Administration and Reporting:** Prepared a final Test Certification Report that described the testing performed for the Oklahoma State Certification Testing project.

**UOCAVA Voting System Testing**
**Client: FVAP/CALIBRE**
**11/2010 – 01/2011**

In 2009, Congress passed the Military and Overseas Voters Empowerment Act (MOVE) instructing the Federal Voting Assistance Program (FVAP) that they may run pilot programs to test the ability of new or emerging technology to better serve uniformed and overseas citizens. MOVE went on to mandate that should FVAP choose to run a pilot program, the Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST) are to help support FVAP by providing best practices or standards to support the projects. In addition, MOVE reiterated the 2004 mandate from Congress requiring EAC to create guidelines to be used by FVAP for the development of a remote electronic voting system.

SLI conducted a onetime test of voting systems to the entire EAC’s Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) “Pilot Program Testing Requirements” date 25 August,
2010. Upon completion of test execution, SLI generated a final test report that documented the testing performed and the associated findings.

**Washington DC Forensic Analysis and Audit of Voting Equipment**

**Client: District of Columbia Board of Elections and Ethics (DCBOEE)**

**9/2010 – 12/2010**

DCBOEE acquired a new voting system to conduct its 2010 September Primary and November General Election. The system is comprised of two hundred Direct Record Electronic (DRE) voting machines, one hundred seventy-five optical scan voting machines, two central count voting units, one Election Management System, and all other peripheral equipment to be used by all voters and accessible to voters with physical, vision and literacy challenges.

SLI was contracted to provide a forensic analysis of the voting system prior to and post the September 2010 primary election as well as the November 2010 general election to ensure (1) that the deployed system was identical to the certified baseline and (2) no improper data entry or security penetration occurred that would affect count accuracy.

SLI first established a system baseline to confirm as-built hash codes and the internal hardware, software, and firmware configuration of the DCBOEE system. After both September and November 2010 elections, SLI conducted a site visit at the DC warehouse to examine randomly selected voting machines. SLI used our NIST-compliant (FIPS certified) hashing algorithms to provide independent verification and validation and confirm that the software and data were not modified in any manner from the originally tested baseline. Analysis was designed to pinpoint any altered files, scripts, or other components and identify the presence of any malicious or altered information. Based on on-site forensic work, a report was delivered to DCBOEE that detailed the results of the election analysis.

**Pennsylvania Department of State QA Assessment of Election Readiness**

**Client: Pennsylvania Department of State**


SLI was contracted to conduct a Quality Assurance assessment of each of the Commonwealth of Pennsylvania’s 67 counties. Current voting system and infrastructure were assessed to develop a concise understanding of the county’s readiness for the November 2004 General election. The assessment process included a final report that summarized the readiness of each county. The assessments provide a detailed analysis of the improvements needed for the current and subsequent elections. Each of the county assessments produced a report that identified the Counties readiness to serve the electorate on Election Day. In addition, the team’s responsibilities included assessments to confirm that Pennsylvania’s own State election code requirements were being satisfied within the assigned Counties and a determination on whether or not those counties were in compliance with the HAVA laws.

The assessment confirmed that Help America Vote Act (HAVA) requirements were being satisfied and that each county was in compliance with regulations. The final assessment and recommendations for improvements were completed and presented to the Commonwealth.
Ohio State Certification of Voting Systems  
Client: Ohio Secretary of State Office  
SLI (then SysTest) was contracted with the Secretary of State in Ohio to conduct an assessment of their current and future voting equipment to be used throughout the state. Services included independent testing and certification of voting equipment to VVSG standards. Ohio general election possible ballot anomalies were reported to the Secretary of State. SLI assisted the Ohio Bureau of Investigation personnel in a forensic investigation into the anomaly.

Minnesota Voting System Assessment  
Client: Minnesota Secretary of State  
SLI completed an independent, third party software evaluation of each of the State of Minnesota’s voting systems to provide a detailed assessment of system security and functional accuracy. The purpose was to certify to the Office of the Secretary of State that the voting system records and counts votes as represented by the voting system vendor. There were three separate reviews performed on each voting system. The results of these activities provided a perspective of the system’s ability to record and count votes as represented by the voting system Vendor. This approach presented additional assurances that the assessment covered all aspects that may influence and affect the vote tabulation and reporting processes, instead of relying on the results of each area individually.

Other examples of recent voting certification and assessment projects include:

<table>
<thead>
<tr>
<th>Project</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES Certification Testing for the 2013 National Election</td>
<td>Republic of the Philippines – COMELEC</td>
</tr>
<tr>
<td>AES Certification Testing for the 2010 National Election</td>
<td>Republic of the Philippines – COMELEC</td>
</tr>
<tr>
<td>California Security Source Code Review</td>
<td>California Secretary of State Office – Election Division</td>
</tr>
<tr>
<td>Dominion Voting Systems Assure 1.3 EAC Federal Certification Testing</td>
<td>Dominion Voting Systems</td>
</tr>
<tr>
<td>Florida Voter Registration System IV&amp;V</td>
<td>Florida Department of State</td>
</tr>
<tr>
<td>New Jersey Central Count Functional Testing</td>
<td>New Jersey Division of Elections</td>
</tr>
<tr>
<td>New Mexico Central Count Functional Testing</td>
<td>New Mexico Secretary of State</td>
</tr>
<tr>
<td>OH Election Technology Assessment/EVEREST Project</td>
<td>Ohio Secretary of State</td>
</tr>
<tr>
<td>Ohio, Cuyahoga County Post Election Test and Analysis</td>
<td>Cuyahoga Ohio</td>
</tr>
</tbody>
</table>
2. Voting Assessment Approach and Process

The respondent’s quote must fully address each of the requirements listed below. In preparing the quote, respondents should consider all activities necessary to meet requirements and the associated costs for each. The selected vendor must meet with key DOS and county staff on the scope of this project and prepare a Statement of Work that includes activities, timelines, and deliverables.

The State is requesting a needs assessment both for the current technology of each county’s voting system, as well as the election related cost and funding for updating/replacing any system. Our assessment for Colorado DOS will include:

- Analysis of each of the county’s current voting systems and services
- Analysis of voting systems certified by Colorado and the EAC
- Analysis of the process for certification
- Analysis and recommendations for the replacement of voting systems
- Estimated equipment costs
- Analysis of funding resources available to counties and State

2.1 Assessment Approach

The SLI approach to a needs assessment for the Colorado Voting System Technology effort includes looking at the broad aspects of the ongoing systems currently in place throughout the State. Our approach will include:

- Project Assessment Kickoff Meeting
- Assessment Process
- Election Officials Interviews
- Weekly Reporting to the DOS
- Final Assessment Report and Presentation
2.1.1 Project Assessment Kickoff Meeting

The assessment begins with a Kickoff Meeting between the SLI Team and the DOS Management. The purpose of the Kickoff Meeting is to introduce the SLI Team to the project and project personnel. It is expected to be our first meeting with the DOS and other oversight partners. Among the key objectives of the meeting are to coordinate the assessment processes and to plan the interaction and scheduling of project status coordination meetings, deliverable reviews, and stakeholder interviews for the assessment period. It is also important for the SLI Team to establish a collaborative relationship with DOS to verify a consistent understanding of roles and responsibilities to assure a complimentary approach to project activities.

This kickoff meeting will occur within one week of the start of our contract. The SLI Project Lead will draft the agenda and distribute it two days prior to the meeting. Any materials that will be discussed will also be provided at that time. The SLI staff who will be involved in the project will attend and explain their role and responsibilities. SLI will serve as the meeting scribe and will document any decisions and action items that are a result of the meeting. The kickoff meeting notes will be distributed the following business day.

2.1.2 Assessment Process

Our approach to the assessment includes:

- Kick-off/Planning Meeting, where SLI will meet with the State to coordinate efforts for the project, as well as granularize each specific goal of the project to a level that ensures understanding and agreement to the final deliverables.
- Review of pertinent documentation available for the project as well as creation and distribution of survey to all counties
- Conduct of surveys and interviews with selected state election staff
- Compilation and assessment of accumulated data
- Report on findings

The Activity Plan table below details the activities within the assessment process:

**Activity Plan**

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kick-off/Planning</td>
<td>7/26/2013</td>
<td>7/26/2013</td>
</tr>
<tr>
<td>Kick-off/Planning meeting</td>
<td>7/26/2013</td>
<td>7/26/2013</td>
</tr>
<tr>
<td>Review of Documentation and Survey Distribution</td>
<td>7/11/2013</td>
<td>7/30/2013</td>
</tr>
<tr>
<td>Current Voting System Analysis</td>
<td>7/11/2013</td>
<td>7/12/2013</td>
</tr>
<tr>
<td>Create County Survey</td>
<td>7/26/2013</td>
<td>7/29/2013</td>
</tr>
</tbody>
</table>
### Task Name

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy County Surveys</td>
<td>7/29/2013</td>
<td>7/30/2013</td>
</tr>
<tr>
<td>Contact manufacturers for cost est.</td>
<td>7/26/2013</td>
<td>7/29/2013</td>
</tr>
<tr>
<td><strong>Compilation and Assessment</strong></td>
<td>7/26/2013</td>
<td>8/23/2013</td>
</tr>
<tr>
<td>Compile County Survey Returns</td>
<td>8/8/2013</td>
<td>8/13/2013</td>
</tr>
<tr>
<td>Assess Current/Future County needs</td>
<td>8/13/2013</td>
<td>8/16/2013</td>
</tr>
<tr>
<td>Gather data on voting systems certification status</td>
<td>7/26/2013</td>
<td>7/29/2013</td>
</tr>
<tr>
<td>Identify State Needs</td>
<td>8/19/2013</td>
<td>8/20/2013</td>
</tr>
<tr>
<td>Complete Replacement Recommendation</td>
<td>8/21/2013</td>
<td>8/23/2013</td>
</tr>
<tr>
<td>Compile cost estimated information</td>
<td>7/29/2013</td>
<td>7/30/2013</td>
</tr>
<tr>
<td>Compile information on funding</td>
<td>7/26/2013</td>
<td>7/30/2013</td>
</tr>
<tr>
<td>Initial report development</td>
<td>8/21/2013</td>
<td>8/26/2013</td>
</tr>
<tr>
<td>Report review</td>
<td>8/26/2013</td>
<td>8/27/2013</td>
</tr>
</tbody>
</table>

### Project Work Site

The services to be provided by SLI personnel will be performed at the SLI facility in Denver, Colorado.

#### 2.1.3 Election Officials Interviews

A central component of our approach involves structured interviews. This consists of preparing pertinent written questions or topics for voting systems and voter services and delivering the Interview Guide to the interviewee three days before the interview appointment. In this way, the project expert has a chance to prepare for the discussion and gather information that needs to be researched. The SLI Team is able to focus upon subject matter questions that have been provided. The outcome is that the staff members interviewed appreciates the opportunity to constructively participate and the information gathered is accurate, pertinent, and useful.

For the voting assessment we plan to Interview the following individuals:

- DOS Executive Director
- DOS Management and Staff
- County Clerks
Questions for the interviews will cover relevant aspects contained in HB 13-303. The data from the interviews will be summarized and provided in an integrated format to the Voting System and Services Assessment Report.

**Interview Guide Tool - SGNaL**

SLI has developed and implemented a structured interview technique that has been used in multiple projects to the advantage of all stakeholders. This cornerstone process consists of preparing pertinent written questions for the topic area and delivering the Interview Guide to the interviewee at least three days before meeting. In this way, the project expert has a chance to prepare for the discussion and information that needs to be researched, and the project Team has a written record of the information to be gathered. Staff interviewed appreciates the opportunity to constructively participate and information gathered is accurate, pertinent, and useful.

Successful implementation of this interview approach over several years has resulted in the creation of the SLI Interview Guide Notes and Library (SGNaL) tool, which contains over 1,200 interview questions covering 21 Project Task Areas. *Exhibit 2.1.3-1, SGNaL: Main Menu* provides a listing of the components of the system that allow SLI to quickly and easily manage the interview process and generate and update specific questionnaires.

*Exhibit 2.1.3-1: SGNaL Main Menu.* This screen allows SLI IV&V Team members to manage our automated tool for conducting structured interviews.

The SGNaL repository allows our team to search for relevant questions that have elicited valuable information in the past, by topic area. The repository also allows the team to easily add new questions based on the requirements defined in the RFQ, components of the voting system and voting services, and/or the unique project circumstances that exist at the time of the interview. *Exhibit 2.1.3-2, SGNaL Interview Maintenance,* provides an example of the screen SLI uses to customize interview questions for specific client needs. After the appropriate questions are selected and the interviewee information has been added to the database, the Interview Guides are automatically generated in Microsoft Word format and are ready to be sent to the...
interviewees. The SIGNaL tool allows the SLI team to focus on the content of the questions being asked rather than the mechanics of creating questionnaires.

Exhibit 2.1.3-2: SIGNaL Interview Maintenance. Questions can be easily selected and interviews generated from within SLI Interview Guide tool.

Interview Guides are designed to produce structured output from the relatively unstructured process of human conversation. Using Interview Guides produces more usable information with less interview time, often saving the project stakeholders from having to revisit discussions on the same topics. The library that is compiled using Interview Guides to collect information on processes and products is an important resource for the project. The SLI interview guides are used by SLI’s Team for all encounters with county election officials to formalize and document the topics, considerations, and observations exchanged in an interview.

2.1.4 Weekly Reporting

The SLI Project Manager is responsible for providing status reports on a weekly basis. Weekly status reports include a concise summary of project schedule and cost status, business and technical issues, and identified project risks. A status reporting process is defined for the project during the initial project planning effort. The status reports document work activities and major accomplishments achieved during the reporting period, in addition to any problems or issues that require attention.

2.1.5 Final Assessment Report and Presentation

Once the assessment is complete the results will be compiled into a final Assessment Report. The following table provides a high level summary of the work components used to prepare and deliver the Voting System Technology Assessment Report.
Assessment Report

Task Description
The assessment report created by the SLI Team evaluates each county's voting systems and the scope of work detailing the RFP. The Assessment Report provides project context and quantitative data on each area analyzed and includes detailed recommendations on how the county and State can improve processes and/or products.

General Approach
The SLI Project Lead submits the assessment report summarizing the observations and assessments developed during the project. The assessment report is organized by technology and cost and funding topics.

Subtasks
- Review of key project deliverables
- Project meetings and reviews
- Interview key project personnel
- Review preliminary finding discussion topics with the DOS prior to completion
- Consolidate findings into the Assessment Report
- Submit Assessment Report to the DOS Project Director, and if so directed, to the Executive Committees and Agency Stakeholders

Timeframe
The assessment report is submitted within 5 weeks of the contract start date, unless a mutually agreed upon alternate date is selected.

Deliverable
Needs Assessment Report on the Voting System Technology

Staff Assigned
SLI Team

SLI will prepare and formally present the findings of the Assessment Report to project stakeholders. The SLI team will respond to questions regarding the methods employed, findings and recommendations of the Voting System needs assessment report. All documentation associated with the presentation will be delivered in hardcopy and electronic media.

3. Voting Technology Assessment

Under the direction of the DOS and in consultation with the Commission, the needs assessment must describe:
A. The current state of technology relating to:

1. Voting Systems. This must include an analysis of voting systems currently used in Colorado and voting systems that may be available that allow counties to conduct elections in accordance with the provisions of HB 13-1303 and the Colorado election code.
2. Certification of Voting Systems. This must include an analysis of voting systems currently certified for use in Colorado, the availability of voting systems that are certified by the U.S. Election Assistance Commission (EAC) but not yet certified in Colorado, and the process and timeline for certifying voting systems that are not currently certified by Colorado, the EAC or any other State.

3. Replacement of Voting Systems. This must include an analysis of counties’ needs for replacing voting systems, the types of systems necessary under the new election model, as well as timing issues based on the elections calendar. This analysis must also consider the implications of the DOS initiative to develop a uniform voting system throughout the state.

The voting technology assessment is the cornerstone of this project. The assessment will allow the DOS and Commission to understand the current status of each individual county, as well as how each fares in comparison to all other counties in the state. The assessment will also provide the DOS and Commission the insight to all the latest systems certified or not certified, with a comparison of the capabilities of each. With the knowledge of the needs for each county coupled with the timing available to implement new systems, the DOS and Commission will be better able to determine the feasibility of developing a uniform voting system throughout the state.

3.1 Current Voting Systems

SLI will compile an assessment of the voting systems (ES&S, Hart, Premier and Sequoia) currently in use throughout the State of Colorado using our Interview Guide Tool - SIGNaL process and other relevant information provided by DOS. Using SLI’s experience in state and federal voting systems, we will develop a set of interview questions to assist in gathering the necessary information and documentation from key personnel. SLI will conduct the reviews and analyze the results. Taking into consideration Colorado’s wishes to move to a uniform voting system throughout the state, SLI will also provide information on other available systems that allow elections to be conducted based on the provision of HB 13-1303 and the Colorado election code.

After gathering the appropriate information, SLI will develop a comprehensive report detailing the systems and configurations in use and provide this to the State.

3.2 Certification of Voting Systems

Analysis of Colorado and EAC-Certified Systems: Based on the information gathered on the current systems in use, SLI will develop a detailed report identifying what systems and configurations are available either that have been certified in the state of Colorado or through the EAC program. In addition, as a current accredited VSTL, SLI will provide an estimate for attaining EAC Certification for the systems that are not yet certified, as well as estimates for certifying systems at the state level.

Process/timeline for systems not currently certified by CO, EAC or any other State: SLI will analyze the overall process, major milestones and any considerations the state will need to be aware of surrounding federal and state based certifications. Using experience gained on other state certification projects, along with quantitative information from current EAC programs, SLI will analyze the process currently in use in Colorado and provide a range of alternatives that may be available to potentially reduce certification cost and schedule without compromising testing integrity or transparency. The estimation will be based on SLI’s expertise in the area of voting
Managing technology risk

system testing and certification along with our in-depth knowledge of the lifecycle for certification.

3.3 Replacement of Voting Systems, including DOS Uniform Voting System Goals

SLI will leverage its extensive knowledge of voting system configurations in performing a thorough analysis of all 64 county’s needs for replacing voting systems. SLI will conduct a detailed analysis of the latest voting systems available, appropriate configurations based on state and local requirements, and latest technology trends in voting systems for consideration. SLI will consider key factors like the age of systems, how many succeeding iterations of patches and code updates have been provided by the vendor, how far out of date the jurisdiction is from the latest version, and failure rates each jurisdiction is experiencing. SLI will also consider the timeframes of system availability and the possible implications of implementing a unified voting system across the state such as; behaviors, architecture capabilities and limitations of the system.

4. Costs and Funding Sources

Under the direction of the DOS and in consultation with the Commission, the needs assessment must describe:
B. The election-related technological costs and funding sources, including:
1. An estimate of necessary equipment costs to conduct elections as described in HB 13-1303 and the Colorado election code
2. An analysis of funding sources that is or may be available for the purchase of new voting systems.

While assessment of the current and available technologies is an important aspect in the exercise of acquiring new systems, equally important is understanding the cost for implementation and where that funding will come from. Utilizing the data gained from the interviews conducted with counties, and understanding the abilities of the currently employed voting systems, SLI will evaluate the cost of replacement of current implementations while maintaining current efficiencies, if not improving on them. Analysis of potential sources of funding available will also be reviewed.

4.1 Estimate of Equipment Costs

As part of the information gathering process and documentation review, SLI will identify the current rate of election data throughput from old equipment to newer models, as well as take into consideration future plans for jurisdictions to determine if a different implementation model will better suit the future plans. This will allow SLI to determine how many new machines are required to replace the current models in order to maintain high efficiency.

SLI will work with the manufacturers for a cost estimation based on the needs assessment for each individual county, as well as on the concept of the statewide uniform voting system, and include the information provided in the detailed reports.
4.2 Analysis of Funding Sources

Based on the information gathered during the interview process, SLI will assist in determining what funding sources may be available to the State. SLI will conduct research on existing funding sources such as HAVA and other state & federal level assistance.

5. Cost Proposal

For purposes of fees and payment, this proposal is priced on a Fixed Price basis, with a total price of $24,000, inclusive of travel or other project related costs.
Memorandum
June 11, 2013

To: The Honorable Scott Gessler, Colorado Secretary of State

From: Debra Johnson, Chair of the Uniform Voting System Advisory Committee

Re: Uniform Voting System Request for Proposal

The Uniform Voting System Advisory Committee has, for the past several meetings, discussed components which we believe should be included in the upcoming Request for Proposal for the Uniform Voting System.

You may recall our discussion, when you met with the Committee, about the overall election system being more than just the elements related to ballot creation, vote casting and vote tabulation. To that end, we have approached the UVS RFP as an opportunity to expand beyond the basic voting system components and move Colorado into a truly Unified Voting System arena.

Our approach is to create a “menu” of component options for various services that local election officials might choose from as they seek to provide specific services. We believe that, while many of the services would be on an “opt in” basis, the option of selecting a State approved vendor for such services is an advantage for those Counties that would choose to provide a specific service. We feel this allows Colorado counties to continue to be forward looking and provides the State with a truly Unified Voting System. Also, many of the vendors may not be able to provide some/all of the services, but addressing the areas allows us all to be informed about possible future uses versus limiting the RFP to current technology.

Attached is a list of the areas we recommend including in the RFP. This list was adopted unanimously by the UVSAC at our May 31, 2013 meeting without objection from any member, after thoroughly discussing each item individually.

If we may provide additional information for your consideration, please feel free to contact me or any of the Committee members.
<table>
<thead>
<tr>
<th>Functionalities Recommended for Inclusion UVS RFP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCORE Integration</td>
</tr>
<tr>
<td>County Ability to Manage Election</td>
</tr>
<tr>
<td>E-Pollbook</td>
</tr>
<tr>
<td>Ballot Creation</td>
</tr>
<tr>
<td>Ballot Printing</td>
</tr>
<tr>
<td>Ballot Mailing</td>
</tr>
<tr>
<td>Ballot Tracking</td>
</tr>
<tr>
<td>Automated Signature Verification</td>
</tr>
<tr>
<td>Ballot Counting</td>
</tr>
<tr>
<td>Digital Ballot Adjudication (Duplicating)</td>
</tr>
<tr>
<td>Electronic Ballot Issue/Receive(UOCAVA)</td>
</tr>
<tr>
<td>Central Count</td>
</tr>
<tr>
<td>Vote Capture/Storage</td>
</tr>
<tr>
<td>Vote Tabulation</td>
</tr>
<tr>
<td>Election Worker Management</td>
</tr>
<tr>
<td>Risk Limiting Audit</td>
</tr>
<tr>
<td>Global Database Change Ability</td>
</tr>
<tr>
<td>Auditability</td>
</tr>
<tr>
<td>Accessibility</td>
</tr>
<tr>
<td>VVPAT Auditable Paper Trail</td>
</tr>
<tr>
<td>Polling Place Survey</td>
</tr>
<tr>
<td>Voter Education</td>
</tr>
<tr>
<td>Issue Tracking</td>
</tr>
<tr>
<td>Pollworker Training</td>
</tr>
</tbody>
</table>
MEMORANDUM

July 18, 2013

The Honorable Scott Gessler,
Colorado Secretary of State
1700 Broadway, Suite 200
Denver, Colorado

Dear Secretary Gessler,

Thank you for taking the time to meet with the UVS Advisory Committee at our July 11, 2013 meeting. We found the discussion most interesting and informative. This letter follows up on that conversation.

At our July 18, 2013 meeting the Committee voted unanimously to request a short delay in issuing the RFP; and, we voted, with only one dissenting vote, to request you to reschedule the issuing of the RFP until October 1, 2013 with a due back date for proposals of December 2, 2013.

We understand others have advocated an indefinite delay, however; we believe this short delay does not negatively impact the project and allows time to fully set the stage for a successful implementation of the Uniform Voting System for several reasons:

1. The delay of a few months does not have a major impact since the county with the most immediate need has found a method to allow it to properly conduct elections through 2014.

2. We can gather experience and needs information based on the new election model in the November 2013 election that will be instructive in evaluating responses to the RFP;

3. We will be able to craft and introduce legislation that will enhance the UVS implementation and perhaps create a source of funding that allows for a timely conversion to a uniform system;

4. It allows sufficient time for the Public Participation Panel to fully gather public input and contribute to the RFP development;

5. It allows us the ability to consider the recommendations of the Colorado Voter Access and Modernized Elections Commission study due September 2.

We encourage you to agree to this short delay in the process so that the Committee can stand with you in encouraging the implementation of the Uniform Voting System.

We hope for a rapid response to this request as the current August 1, 2013 deadline is very near.

Respectfully,

Debra Johnson, Chair, Uniform Voting System Advisory Committee
Overview for Commission of Security Policies, Practices and Controls – prepared by Trevor Timmons

Presented at the July 15, 2013 meeting of the Commission

Visible to Users
1. SANS (Systems Administration, Networking & Security) Institute basic security training (Securing the Human) for all county users. **Standard practice.**
2. Login and Password authentication **Standard practice, assuming there is a strong password policy.**
3. Multi-factor Authentication (Entrust grid card example), currently in county pilot testing. **Best practice.**
4. User Policies (Acceptable Use Policy) for each regular user of SCORE. **Standard practice.**
5. Wireless security standard for any potential use of wireless networking in elections-related scenarios. **Standard practice.**

Mostly Invisible to Users

Current
1. SANS Secure Coding training for development staff. **Best practice if done regularly.**
2. Human-based vulnerability testing (so-called “white hat” attacks). **Best practice.**
3. Automated vulnerability testing. **Standard practice.**
4. Patch and vulnerability management scanning and review. **Standard practice.**
5. IDS/IPS systems. **Intrusion Detection System/Intrusion Prevention System. Standard practice.**
6. Geographic IP blocking (limited to CONUS). **Best practice.**
7. One-day window for activation of VC (Vote Center) users. **Best practice.**
8. Centralized log collection and monitoring. **Standard practice.**

Future
1. Web Application Firewall activity. **Standard practice.**
2. Web volume blocks. **Standard practice.**
3. More modern and user-friendly system for secure file/information transfer. **Standard practice.**

Commissioners,

To provide some perspective, I have separated the security items above into two groups:

1. **Standard practices.** These are security steps that are generally considered an industry standard practice in the sense that they form the basis of any reasonable security program. Much like you would expect a car today to have airbags and anti-lock brakes, you should expect a program such as SCORE to use automated vulnerability testing and maintain centralized logs.
2. **Best practices.** These are security steps that are generally considered an industry best practice in the sense that they provide an extra degree of security. To extend my car analogy, you don’t necessarily need features such as rain-sensing wipers and a backup camera, but you might value them enough to pay the added cost. I’ll explain the best practices individually below:
   a. **Multi-factor authentication.** A login (username + password) is an example of single-factor authentication. The user is relying on something they know to gain access to the system. You can force the user to create a complex password and change it regularly, but you’re still relying on a single factor. The vast majority of systems today use single-factor authentication.
Multi-factor authentication, as the phrase implies, adds another factor. In the case of SCORE, Trevor shared a grid card with numbers and letters. When a user logs into the system, she will be prompted to enter a code from the grid card (in addition to her username and password). Now the user is relying on something they have (grid card) as well as something they know (username and password) in order to gain access to the system. This type of authentication is often used by financial institutions to help prevent fraud. At OIT we use electronic tokens that generate a code to help prevent unauthorized access to our network.

b. **Secure coding training.** The nature of computer programming is that there are usually several ways to accomplish the same thing, but only one way to maximize security. I compare it to an Excel spreadsheet – there are several ways to get to the bottom line on an income statement, but only one formula that is the most efficient. Most companies try to hire programmers with secure coding experience, but the best practice is to provide this type of training on a regular basis to keep up with new threats.

c. **Human-based vulnerability testing.** Nearly all vulnerability testing is done using software programs that scan an application for known weaknesses. Such programs can be scheduled to run during non-peak hours and perform literally hundreds of tests in a very short period of time. However, an automated program can only test for weaknesses that have been accounted for in its programming. One example would be to check for the default password on an administrative login. A human, while much slower than an automated program, can be much more creative.

d. **Geographic IP blocking.** You can purchase databases or use lookup services that identify the approximate geographic area associated with an IP address (the address of a device such as a server on the Internet). Since it’s reasonable to assume that SCORE users are in the US, it’s also reasonable to assume that someone attempting to access SCORE from outside of the US is not an authorized user. In this case, blocking traffic from IP addresses that are known to be outside of the continental US adds a degree of security.

e. **One-day activation window.** Putting a time constraint on when someone is able to activate their user account isn’t necessary, but it limits the amount of time that a hacker can use to exploit the system. It also removes the possibility of having a pool of inactive accounts build up over time.

When you add all of the items together, CDOS has a very strong set of security policies and practices that they apply to their staff and the SCORE system. However, there is a third element to consider – the end user. I have had an initial discussion with David Bessen, the CIO for Arapahoe County. He is in the process of gathering information on how they secure the end user’s PC and should have that back to me this week.
SCORE Security Controls

Contents
SCORE Security Controls ........................................................................................................... 1

CURRENT SECURITY CONTROLS ......................................................................................... 2
Securing the Human Training ................................................................................................. 2
Login & Password Authentication ......................................................................................... 2
Multi-Factor/Two-Factor Authentication .............................................................................. 2
User Policies .......................................................................................................................... 3
Authorized User & Monitoring Agreement – Click Through .................................................. 3
Wireless Security Standards ................................................................................................. 4
SANS Secure Code Training .................................................................................................. 4
Human-based vulnerability testing (so-called “white hat” attacks) ..................................... 5
Patch and vulnerability management scanning and review ................................................... 5
IDS/IPS systems ...................................................................................................................... 5
Geographic IP blocking (limited to CONUS) ....................................................................... 5
One day window for activation of VC (Vote Center) users ................................................. 5
Centralized log collection and monitoring .......................................................................... 5
Security Professionals throughout organization .................................................................... 5
Future Security Controls ....................................................................................................... 6
Web Application Firewall, Web Volume Blocks, DDOS Attacks & IP Enforcer .................... 6
More modern and user-friendly system for secure file/information transfer ....................... 6
Detailed IP and machine identity tagging ........................................................................... 6
Improved IDS/IPS systems .................................................................................................... 6
CURRENT SECURITY CONTROLS

Securing the Human Training
Currently 286 County User Administrators are enrolled in the SANS Securing the Human training. Out of the 286 County User Administrators 274 have completed the training.

<table>
<thead>
<tr>
<th>Score</th>
<th>Enrolled</th>
<th>Not Started</th>
<th>In Progress</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>286</td>
<td>9</td>
<td>3</td>
<td>274</td>
<td></td>
</tr>
</tbody>
</table>

The very extensive training takes approximately two hours to complete and covers every relevant topic related to end user security practices. The topics cover everything from how to stay safe when browsing the Internet to the proper security configuration requirements for your workstation.

<table>
<thead>
<tr>
<th>Introduction</th>
<th>IT Staff (Optional)</th>
<th>Gramm Leach Bliley - EDU (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>You Are The Target</td>
<td>Physical Security</td>
<td>Gramm Leach Bliley - FIN (Optional)</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Protecting Your Personal Computer</td>
<td>The Red Flags Rule (Optional)</td>
</tr>
<tr>
<td>Email and IM</td>
<td>Protecting Your Home Network</td>
<td>Ethics (Optional)</td>
</tr>
<tr>
<td>Browsing</td>
<td>Protecting Your Kids Online</td>
<td>Advanced Persistent Threat (Optional)</td>
</tr>
<tr>
<td>Social Networking</td>
<td>Hacked</td>
<td>Cloud (Optional)</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td>Senior Leadership (Optional)</td>
<td>International Traffic in Arms Regulations (Optional)</td>
</tr>
<tr>
<td>Passwords</td>
<td>PCI DSS (Optional)</td>
<td>Data Retention (Optional)</td>
</tr>
<tr>
<td>Encryption</td>
<td>FERPA (Optional)</td>
<td>Social Security Numbers (New Module - Optional)</td>
</tr>
<tr>
<td>Data Protection</td>
<td>HIPAA (Optional)</td>
<td>END</td>
</tr>
<tr>
<td>Data Destruction</td>
<td>PII</td>
<td></td>
</tr>
<tr>
<td>Wi-Fi Security</td>
<td>Criminal Justice (Optional)</td>
<td></td>
</tr>
<tr>
<td>Working Remotely</td>
<td>Federal Tax Information (Optional)</td>
<td></td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insider Threat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Help Desk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Login & Password Authentication

➢ All new SCORE passwords are set to a unique value meeting password complexity requirements.
  o At least 8 characters
  o Containing 3 out of 4 of the following:
    ▪ Upper case letter
    ▪ Lower case letter
    ▪ Number
    ▪ Symbol

➢ Users are required to change their passwords every 90 days.
➢ Accounts that have been inactive for one year or more are removed from the system.

Multi-Factor/Two-Factor Authentication
User names and passwords do not provide the level of protection needed for sensitive information. Another factor of authentication has become necessary as hackers have become more skilled and targeted attacks sponsored by foreign states against critical government systems have become common.
Two-Factor authentication requires two out of three of the following to login to a system:

- Something you know (usernames and passwords)
- Something you have (grid card, token)
- Something you are (Biometrics such as fingerprint readers or retinal scans)

SCORE Customer Support is rolling out Grid Cards to the counties. Each county will also have the option to purchase tokens from Entrust.

User Policies
Please see attached existing and future draft End User Policies for SCORE.

Authorized User & Monitoring Agreement – Click Through
All users must agree to the following before logging in.

“This system is the property of the Colorado Department of State (CDOS) and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to administrative action, civil enforcement, and criminal prosecution as applicable to the offense.

This system contains personal identifying information that is sensitive and shall not be disclosed to unauthorized persons. Protected information includes but is not limited to social security numbers, month and day of birth, driver’s license numbers, and signature images. Disclosure of protected information to unauthorized persons is strictly prohibited.

Computing devices accessing this system shall have up-to-date anti-virus with real time protection enabled, host level firewalls, up-to-date software patches and be configured to meet security best practices set by the County and State.

CDOS authorized personnel may monitor, record, and copy any activity or communication on this system and retrieve any information stored within this system.

By accessing and using this system, you consent to these terms.”
Wireless Security Standards
Please see attached wireless standards provided to all counties.

SANS Secure Code Training
“Critical software systems, designed to enable business, are often at the root of many headlines about data breaches and corporate hacks. The most common attacks are often caused by simple mistakes that occur while software is being developed and deployed.

By educating everyone involved in the software development process, including developers, architects, managers, testers, business owners and partners, you reduce the chances that your organization will become a victim of today’s data security threats and ensure your team can properly build defensible applications from the start. STH.Developer provides the pinpoint software security awareness training that your team needs when they need it most, from the comfort of their own desks.” – SANS Institute

All CDOS developers will be required to complete a new training course provided by SANS called “Securing the Developer” covering the following categories.

<table>
<thead>
<tr>
<th>Introduction - Developer Injection</th>
<th>Session Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient Transport Layer Protection</td>
<td>Insecure Direct Object Reference</td>
</tr>
<tr>
<td>Invalidated Redirects &amp; Forwards</td>
<td>Cross Site Request Forgery</td>
</tr>
<tr>
<td>Cross-Site Scripting Authentication</td>
<td>Security Misconfiguration</td>
</tr>
<tr>
<td></td>
<td>Insecure Cryptographic Storage</td>
</tr>
<tr>
<td></td>
<td>URL Access Failure</td>
</tr>
</tbody>
</table>

In addition to the Securing the Developer class most of our developers have taken 40 hours of either SANS .NET or Java secure coding classes. Two more developers on the SCORE development team will complete the .NET secure coding class this year. The class covers the following security topics.

- Web application attacks and defenses
- SQL Injection
  (including LDAP, XML, and Xpath injection)
- Cross-site scripting
- Cross-site request forgery
- Parameter manipulation
- Numeric overflow
- Web application proxies
- Using Fiddler
- Assemblies
- Strong name vs weak named
- Global Assembly Cache (GAC)
- Authentication
- IIS / ASP.Net pluggable authentication architecture
- Basic, digest, forms, and windows authentication
- Authorization, OS security, and impersonation

- .NET encryption services
- Encryption principals
- Securing communications
- Protecting data at rest
- .NET built in security features
- Limited protections against cross-site request forgery, cross-site scripting, response splitting
- Exception handling and audit logging
- Security in SDL/C
- Static analysis overview
- Dynamic analysis overview
- Threat modeling
- Code-review techniques

**Human-based vulnerability testing (so-called “white hat” attacks)**
CDOS contracts with one of the top web application testing companies in the World. They perform both automated and dynamic best web application testing in order to find any security weaknesses related to our web application before an attacker does.

Testing is performed weekly with some of the best White Hat hackers in the world.

**Patch and vulnerability management scanning and review**
Complete patch and vulnerability management scans are performed every week against all CDOS systems, including SCORE. Any vulnerabilities found are then reviewed and rated according to risk in order to determine an acceptable timeline for mitigation.

**IDS/IPS systems**
SCORE has an active network IDS/IPS system in place at both data centers. Logs from these systems are reviewed by both DRC as a part of their contract and CDOS personnel on a daily basis. Two additional IDS/IPS systems are currently being configured and deployed for even more detailed detection in the near future.

**Geographic IP blocking (limited to CONUS)**
All IP address spaced located outside of the United States are currently blocked. This dramatically lowers the number of attacks experienced by SCORE on a daily basis and allows for our engineers to focus on the true threats to the environment. Additional controls are being considered after the grid card deployment to take this security control to the next level.

**One day window for activation of VC (Vote Center) users**
The Vote Center web application is only available on Election Day. This significantly lowers the possibility of the application being attacked successfully. With the passage of HB13-1303 the vote center application will no longer be used. Requirements surrounding HB13-1303 have not been established yet.

**Centralized log collection and monitoring**
All systems, network and security logs are collected and secured centrally. This ensures that the logs will not be tampered with on an individual system and allows for professional log review by security professionals on both the DRC and CDOS staff.

**Security Professionals throughout organization**
Security systems can't detect a successful intrusion and adapt to new attacks if properly trained security professionals are not available to review logs, update systems and implement new controls. Currently CDOS and DRC employ several certified security and network professionals.

- Certified Information Systems Security Professionals (CISSP) – 2
- Certified Incident Handlers (GCIH)- 2
- Security+ Certified Engineers – 3
- Network+ Certified Engineers – 1
Cisco Certified Internet Engineers (CCIE)- 1

In addition to the certified engineers above, several of our engineers have completed the course work and are currently preparing to take additional certification exams for both the CISSP and Cisco networking certifications.

Future Security Controls

Web Application Firewall, Web Volume Blocks, DDOS Attacks & IP Enforcer
Currently the Voter registration application is protected by a Web Application Firewall. Any future web applications implemented on the SCORE systems will be protected as well.

“A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked.” – OWASP

Along with standard web application protections automatic mechanisms to block IP addresses attempting denial of service, web scraping, or continual web attacks are blocked automatically.

More modern and user-friendly system for secure file/information transfer
A more accessible and manageable means to transfer sensitive files is needed. On July 1st CDOS received approval to purchase a more secure file transfer service that will integrate with Outlook, SharePoint, and allow for easier secure group collaboration.

Detailed IP and machine identity tagging
After two-factor authentication is fully deployed in the Counties additional controls will be considered. The possibility of locking down the system to only county IP addresses, utilizing device authentication and end-point controls will be considered.

Improved IDS/IPS systems
An additional network IDS/IPS as well as a host based IDS/IPS system is ready for deployment. These will be put in place to provide a better defense in-depth posture over the next six months.
Statewide Colorado Registration and Election system (SCORE) 
Acceptable Use Policy

PURPOSE:
The Score system maintains sensitive information that is proprietary information and as such requires protection under the provisions of the Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974). The purpose of this policy is to establish a standard to protect information received; collected, developed through or in the use of the Colorado Department of State SCORE system and that this information is protected from unauthorized access, use, or disclosure.

SCOPE:
This policy applies to employees, contractors, consultants, temporaries, and other workers of the State of Colorado, including all personnel affiliated with third parties that access and/or use the SCORE system and any associated equipment that is owned or leased by the State of Colorado that is used to manage, access and or monitor the SCORE system. All Colorado SCORE users must sign and agree with this policy. [Reference Colorado Information Security Act (C.R.S. 24-37.5, Part 4) and State of Colorado Cyber Security Program P-CCSP 001, dated December 20, 2006]

INDIVIDUAL RESPONSIBILITIES:
Users of the SCORE system are hereby subject to and shall comply with the following standards and provisions for acceptable use:

- Access, use or disclosure of sensitive information must be necessary to the performance of the responsible individual’s job duties and function and must be expressly authorized. Unauthorized access to, use of, or disclosure of sensitive information is strictly prohibited.

- Sensitive information shall not be displayed or otherwise made available or accessible to unauthorized persons. This rule applies, without limitation, to Social Security Numbers (SSN) contained in document images on workstations, and to other personal and or confidential information, such as Date of Birth (DOB), Driver License Number etc.

- Users and their representative departments are responsible to ensure proper encryption and handling of sensitive voter information that is downloaded to portable devices such as laptops, PDA’s, memory cards etc.

- Sanctioned users of the SCORE system are responsible for ensuring proper workstation management and configuration, as such should:
  - Ensure sensitive information is not displayed on a computer screen, in a manner such that unauthorized persons may view the sensitive information.
  - Ensure firewall services including updated versions of antivirus and anti-spyware applications are safeguarding the SCORE access terminal/Workstations.
  - Ensure workstation maintenance activities are authorized and observed.
  - Ensure automatic screen saver lockout is active so that your machine goes to screensaver mode after 10 minutes of inactivity, requiring your password to gain re-entry.
  - Practice safe surfing habits. Casually ‘browsing’ the internet, is prohibited
  - Do not send or download any software including shareware, freeware, or browser controls unless authorized to do so.
  - If a systems performance becomes erratic, you suspect it has been tampered with, or the local virus protection software finds an infection contact the SCORE help desk immediately. System performance or erratic behavior often indicates a Malware infection such as a virus or Trojan.

- Failing to comply or intentional abuse of this policy may result in the loss of access to the SCORE system and could include disciplinary action up to and including, termination, and/or prosecution under the provisions of State and Federal law.

INITIALS

SCORE Cyber Security Policy 002
CDOS Rev 1.0
Page 1 of 2
2008-09-29
Statewide Colorado Registration and Election system (SCORE)
Acceptable Use Policy

DEFINITIONS:

Sensitive Information - As referenced in the provisions of this policy, sensitive information is any and all data or information, in any format, received, collected or developed by the Secretary of State or the Department of State SCORE System up to and including individual identity. The information maintained in the SCORE system is therefore considered proprietary and confidential information that requires protection from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information.

USER ACKNOWLEDGEMENT:
I hereby certify that I have reviewed the SCORE Acceptable Use Policy, and understand the restrictions and regulations contained therein. By signing this form, I affirm my willingness to abide by the SCORE Authorized Use Policy, procedures and guidelines. I agree to treat all information as sensitive and will not disclose any information to anyone without the express permission of the SCORE managing authority. I acknowledge receipt of a copy of this policy. If I have any questions regarding this policy, I will obtain clarification from my supervisor before taking any action.

Name Printed: ___________________________ County: ___________________________

Signature: ___________________________ Date: ___________________________

INITIALS

SCORE Cyber Security Policy 002
CDOS Rev 1.0
Page 2 of 2
2008-09-29
Statewide Colorado Registration and Election system (SCORE) Password Application Form

PURPOSE:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the SCORE system and related sensitive information. As such, all employees including contractors and vendors with access to SCORE system are responsible for taking the appropriate steps, as outlined below, to obtain, select and secure their passwords. The purpose of this policy is intended to reduce the risk of unauthorized access by establishing standards for users of the SCORE system in obtaining and maintaining a password for access to the SCORE system.

SCOPE:

This policy applies to employees, contractors, consultants, temporaries, and other workers of the State of Colorado, including all personnel affiliated with third parties that access and/or use the SCORE system and any associated equipment that is owned or leased by the State of Colorado that is used to manage, access and or monitor the SCORE system. All Colorado SCORE users must sign and agree with this policy.

INDIVIDUAL RESPONSIBILITY:

Password Requirements - Strong passwords are required to log into the SCORE system. Strong passwords must:

1) Be at least eight characters in length
2) Be changed at least every 90 days.
3) Require the use of three out of four of the following:
   - Capital letters
   - Lower case letters
   - Numbers
   - Special characters

PASSWORD CREATION GUIDELINES:

The following password creation guidelines are based upon best practices for protecting sensitive information and information systems:

1) Passwords must contain at least one alphabetic and one numeric character.
2) Passwords should use digits and punctuation characters as well as letters e.g., 0-9, ! @/#$%^&*()_+-=\{\}[\];\:,<??),/)
3) Passwords must be significantly different from previous passwords.
4) Passwords should not be the same as the user ID.
5) Passwords should not start or end with the initials of the person issued the user ID.
6) Passwords should not include the first, middle, or last name of the person issued the user ID.
7) Passwords should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, months, dates, family member names or street addresses.
8) Passwords should not consist of words that can be found in a dictionary, even if you are substituting numbers for letters, such as “zero” for the letter O.

PASSWORD MANAGEMENT:

Penalties for sharing passwords can be severe and could include disciplinary action up to and including loss of access to the SCORE application, termination, and/or prosecution under the provisions of State and Federal law. The following password management standards are based upon industry best practices and key to proper implementation of your responsibilities as a SCORE user:

- User ID’s and passwords are to be kept strictly confidential. Do not give or share your ID or password to anyone, including your supervisor.
- Do not write your ID and/or password down as you have no control over those who may find it and use it inappropriately. Each user is responsible for all actions associated with their Logon ID and password and will be held accountable for any improprieties regarding its use.

INITIAL

SCORE Cyber Security Policy 001
CDOS Rev 1.0
Page 1 of 2
2008-09-30
Statewide Colorado Registration and Election system (SCORE)  
Acceptable Use Policy DRAFT

PURPOSE:
The Score system maintains sensitive information that is proprietary information and as such requires protection. The purpose of this policy is to establish a standard to protect sensitive information contained in the Colorado Department of State SCORE system.

SCOPE:
This policy applies to employees, contractors, consultants, temporaries, and other workers of the State of Colorado, including all personnel affiliated with third parties that access and/or use the SCORE system and any associated equipment that is owned or leased by the State of Colorado that is used to manage, access and or monitor the SCORE system. All Colorado SCORE users must sign and agree with this policy. [Reference Colorado Information Security Act (C.R.S. 24-37.5, Part 4) and State of Colorado Cyber Security Program P-CCSP 001, dated December 20, 2006]

INDIVIDUAL RESPONSIBILITIES:
An individual accessing the SCORE system must comply with the following standards and provisions for acceptable use:

- Access, use or disclosure of sensitive information must be necessary to the performance of the responsible individual’s job duties and function and must be expressly authorized. Unauthorized access to, use of, or disclosure of sensitive information is strictly prohibited.
- Sensitive information must not be displayed or otherwise made available or accessible to unauthorized persons. This rule applies, without limitation, to Social Security Numbers (SSN) contained in document images on workstations, and to other personal and or confidential information, such as Date of Birth (DOB), Driver License Number, etc.
- Users and their representative departments are responsible to ensure proper encryption and handling of sensitive voter information that is downloaded to portable devices such as laptops, PDA’s, memory cards etc.
- Sanctioned users of the SCORE system are responsible for ensuring proper workstation management and configuration, as such should:
  o Ensure sensitive information is not displayed on a computer screen, in a manner such that unauthorized persons may view the sensitive information.
  o Ensure firewall services including updated versions of antivirus and anti-spyware applications are safeguarding the SCORE access terminal/Workstations.
  o Verify that a complete system anti-virus scan is performed once per week.
  o Ensure workstation maintenance activities are authorized and observed.
  o Ensure automatic screen saver lockout is active so that your machine goes to screensaver mode after 15 minutes of inactivity; requiring your password to gain re-entry.
  o Practice safe surfing habits. Casually ‘browsing’ the internet, is prohibited.
  o Ensure systems and third party software are fully patched or have proper mitigating controls in place including the following:
    ▪ Operating Systems
    ▪ Adobe Reader, Flash and Shockwave
    ▪ Internet Explorer, Firefox, Chrome and other Web Browsers
    ▪ All versions of Java on the machine.
  o Do not send or download any software including shareware, freeware, or browser controls unless authorized to do so.
  o All systems are hardened to meet CIS (Center for Internet Security) requirements.

INITIALS
Statewide Colorado Registration and Election system (SCORE)
Acceptable Use Policy DRAFT

- If a systems performance becomes erratic, you suspect it has been tampered with, or the local virus protection software finds an infection contact the SCORE help desk immediately. System performance or erratic behavior often indicates a Malware infection such as a virus or Trojan.

- Failing to comply or intentional abuse of this policy may result in the loss of access to the SCORE system and could include disciplinary action up to and including, termination, and/or prosecution under the provisions of State and Federal law.

DEFINITIONS:

**Sensitive Information** - As referenced in the provisions of this policy, sensitive information is any and all data or information, in any format, received, collected or developed by the Secretary of State or the Department of State SCORE System up to and including individual identity. The information maintained in the SCORE system is therefore considered proprietary and confidential information that requires protection from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information.

USER ACKNOWLEDGEMENT:

I hereby certify that I have reviewed the SCORE Acceptable Use Policy, and understand the restrictions and regulations contained therein. By signing this form, I affirm my willingness to abide by the SCORE Authorized Use Policy, procedures and guidelines. I agree to treat all information as sensitive and will not disclose any information to anyone without the express permission of the SCORE managing authority. I acknowledge receipt of a copy of this policy. If I have any questions regarding this policy, I will obtain clarification from my supervisor before taking any action.

Name Printed: ___________________________ County: ___________________________

Signature: ___________________________ Date: ___________________________

SCORE Cyber Security Policy 002
CDOS Rev 1.1

Page 2 of 2
2013-07-26
TO: All County Elections IT Staff

RE: CLARIFICATION ABOUT WIRELESS TECHNOLOGIES USED AT POLLING PLACES:

This communication will discuss the State's guidelines for using wireless technologies at polling place locations for the Primary and General elections.

One assumption stands for both 802.11 and Cellular technologies: Both elections applications, SCORE II – Citrix and SCORE II – Vote Center, use secured host-to-host encryption, such as SSL.

For the purposes of using 802.11 wireless networking at a polling place, the Office of Cyber Security recommends:

1. The use of WPA with Pre-shared keys at a minimum*.
2. Pre-shared keys have a minimum of a 21 character passphrase.
3. The Wireless Access Point is physically secured to deter tampering.
4. The Wireless Access Point is owned and maintained by the county or county contractors
5. Computers are configured NOT to "automatically connect to non-preferred networks".
6. Computers are up to date on Operating System and Software patches.
7. Computers have a local firewall installed and configured appropriately for the environment.
8. Computers have up-to-date anti-virus and anti-spyware software installed and configured appropriately.
9. Computers are not configured to "bridge" networks or "route" or "forward" network traffic.

* - Where practical, implementing WPA-2 with TKIP or CCMP using 802.1X protocols is the preferred security configuration for wireless access points.

Since there are no commonly known vulnerabilities inherent in CDPD, CDMA, and GPRS network authentication and transmission security methods as well as the lack of configurable options on an end device, the following recommendations are focused on the Computer.

For the purposes of using "air-cards" or other cellular technologies at a polling place, the Office of Cyber Security recommends:

1. Computers are configured to disable other wireless network adapters except the cellular modem / adapter.
2. Computers are up to date on Operating System and Software patches.
3. Computers have a local firewall installed and configured appropriately for the environment.
4. Computers have up-to-date anti-virus and anti-spyware software installed and configured appropriately.
5. Computers are not configured to "bridge" networks or "route" or "forward" network traffic.
SANS Software Security Curriculum

**Defense**
- DEV522: Defending Web Applications Security Essentials GWEB

**Secure Coding**
- JAVA
  - DEV541: Secure Coding in Java/JEE GSSP-JAVA
- .NET
  - DEV544: Secure Coding in .NET GSSP-.NET

**Attack**
- SEC542: Web App Pen Testing and Ethical Hacking GWAPT

New!
- SEC642: Advanced Web App Pen Testing and Ethical Hacking

Additional Software Security Courses
http://software-security.sans.org

Curriculum by Job Role

<table>
<thead>
<tr>
<th>Job / Role in Organization</th>
<th>Recommended Curriculum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developer</td>
<td>DEV522: Defending Web Applications Security Essentials GWEB All DEV courses cover the OWASP Top 10 and CWE/SANS Top 25 Software Errors</td>
</tr>
<tr>
<td>Senior Developer/Technical Team Lead</td>
<td>DEV522: Defending Web Applications Security Essentials GWEB OR DEV544: Secure Coding in .NET GSSP-.NET</td>
</tr>
<tr>
<td>Architect</td>
<td>DEV522: Defending Web Applications Security Essentials GWEB OR DEV544: Secure Coding in .NET GSSP-.NET</td>
</tr>
<tr>
<td>Manager</td>
<td>DEV522: Defending Web Applications Security Essentials GWEB</td>
</tr>
</tbody>
</table>

For more information on these courses, visit http://software-security.sans.org
The course to take to learn Secure Coding in Java!

Great programmers have traditionally distinguished themselves by the elegance, effectiveness, and reliability of their code. That's still true, but elegance, effectiveness, and reliability have now been joined by security. Major financial institutions and government agencies have informed their internal development teams and outsourcers that programmers must demonstrate mastery of secure coding skills and knowledge through reliable third-party testing or lose their right to work on assignments for those organizations. More software buyers are joining the movement every week. Such buyer and management demands create an immediate response from programmers, “Where can I learn what is meant by secure coding?” This unique SANS course allows you to bone up on the skills and knowledge required to prevent your applications from getting hacked.

What Does the Course Cover?

This is a comprehensive course covering a huge set of skills and knowledge. It's not a high-level theory course. It's about real programming. In this course you will examine actual code, work with real tools, build applications, and gain confidence in the resources you need for the journey to improving the security of Java applications.

Rather than teaching students to use a set of tools, we're teaching students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors.

The class culminates in a Secure Development Challenge where you perform a security review of a real-world open source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that you have learned in class, implement fixes for these issues.

What You Will Learn

- Web Application Attacks and Defenses
  - Cross-site scripting (XSS)
  - Cross-site request forgeries (CSRF) - SQL injection
  - HTTP response splitting
  - Parameter manipulation
  - Directory Traversal
  - Web application proxies
  - Using Paras
  - Authentication
  - Basic & forms based authentication
  - Client certificate authentication
  - Spring security
  - Session Management
  - SAttacks, defense, and best practices

- Encryption
- JSS
g- JCA
- Secure password storage
- Logging & error handling
- Race conditions
- Java Security Manager
- Jar Signing
- Security in SDL
- Static Analysis Overview
- Dynamic Testing Overview
- Code Review techniques
The course for Secure Coding in .NET!

ASP.NET and the .NET framework have provided web developers with tools that allow them an unprecedented degree of flexibility and productivity. On the other hand, these sophisticated tools make it easier than ever to miss the little details that allow security vulnerabilities to creep into an application. Since ASP.NET, 2.0 Microsoft has done a fantastic job of integrating security into the ASP.NET framework, but the onus is still on application developers to understand the limitations of the framework and ensure that their own code is secure.

During this four-day course we will analyze the defensive strategies and technical underpinnings of the ASP.NET framework and learn where, as a developer, you can leverage defensive technologies in the framework, where you need to build security in by hand. We'll also examine strategies for building applications that will be secure both today and in the future.

Rather than focusing on traditional web attacks from the attacker's perspective, this class will show developers first how to think like an attacker, and will then focus on the latest defensive techniques specific to the ASP.NET environment. The emphasis of the class is a hands-on examination of the practical aspects of securing .NET applications during development.

Have you ever wondered if ASP.NET Request Validation is effective? Have you been concerned that XML web services might be introducing unexamined security issues into your application? Should you feel uneasy relying solely on the security controls built into the ASP.NET framework? Secure Coding in ASP.NET will answer these questions and far more.

What You Will Learn

- Web application attacks and defenses
  - SQL Injection
    (including LDAP, XML, and Xpath injection)
  - Cross-site scripting
  - Cross-site request forgery
  - Parameter manipulation
  - Numeric overflow
  - Web application proxies
  - Using Fiddler
  - Assemblies
  - Strong name vs weak named
  - Global Assembly Cache (GAC)
  - Authentication
    - IIS / ASP.Net pluggable authentication architecture
    - Basic, digest, forms, and windows authentication
    - Authorization, OS security, and impersonation

- NET encryption services
  - Encryption principals
  - Securing communications
  - Protecting data at rest
  - NET built in security features
    - Limited protections against cross-site request forgery, cross-site scripting, response splitting
  - Exception handling and audit logging
  - Security in SDLC
    - Static analysis overview
    - Dynamic analysis overview
    - Threat modeling
    - Code-review techniques
Assess Your Web Apps in Depth

Web applications are a major point of vulnerability in organizations today. Web app holes have resulted in the theft of millions of credit cards, major financial and reputational damage for hundreds of enterprises, and even the compromise of thousands of browsing machines that visited Web sites altered by attackers. In this intermediate to advanced level class, you’ll learn the art of exploiting Web applications so you can find flaws in your enterprise’s Web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, you will be taught the four-step process for Web application penetration testing. You will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. You will utilize cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment. And you will explore various other Web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen. You will learn the tools and methods of the attacker, so that you can be a powerful defender.

On day one, we will study the attacker’s view of the Web as well as learn an attack methodology and how the pen-tester uses JavaScript within the test. On day two, we will study the art of reconnaissance, specifically targeted to Web applications. We will also examine the mapping phase as we interact with a real application to determine its internal structure. During day three we will continue our test by starting the discovery phase using the information we gathered on day two. We will focus on application/server-side discovery. On day four we will continue discovery, focusing on client-side portions of the application, such as Flash objects and Java applets. On day five, we will move into the final stage of exploitation. Students will use advanced exploitation methods to gain further access within the application. Day six will be a Capture the Flag event where the students will be able to use the methodology and techniques explored during class to find and exploit the vulnerabilities within an intranet site.

Throughout the class, you will learn the context behind the attacks so that you intuitively understand the real-life applications of our exploitation. In the end, you will be able to assess your own organization’s Web applications to find some of the most common and damaging Web application vulnerabilities today.

By knowing your enemy, you can defeat your enemy. General security practitioners, as well as Web site designers, architects, and developers, will benefit from learning the practical art of Web application penetration testing in this class.

From the Author

Testing the security of Web applications is not as simple as just knowing what SQL injection and cross-site scripting mean. Successful testers understand that methodical, thorough testing is the best means of finding the vulnerabilities within the applications. This requires a deep understanding of how Web applications work and what attack vectors are available. This course provides that understanding by examining the various parts of a web application penetration. When teaching the class, I especially enjoy the use of real-world exercises and the in-depth exploration of Web penetration testing. - Kevin Johnson
This course is designed to teach you the advanced skills and techniques required to test web applications today. This advanced pen testing course uses a combination of lecture, real-world experiences, and hands-on exercises to educate you in the techniques used to test the security of enterprise applications. The final day of the course culminates in a Capture the Flag (CTF) event, which tests the knowledge you will have acquired the previous five days.

We will begin by exploring specific techniques and attacks to which applications are vulnerable. These techniques and attacks use advanced ideas and skills to exploit the system through various controls and protections. This learning will be accomplished through lectures and exercises using real-world applications.

We will then explore encryption as it relates to web applications. You will learn how encryption works as well as techniques to identify the type of encryption in use within the application. Additionally, you will learn methods for exploiting or abusing this encryption, again through lecture and labs.

The next day of class will focus on how to identify web application firewalls, filtering, and other protection techniques. You will then learn methods to bypass these controls in order to exploit the system. You'll also gain skills in exploiting the control itself to further the evaluation of the security within the application.

Following these general exploits, you will learn techniques that target specific enterprise applications. You will attack systems such as content management and ticketing systems. We will explore the risks and flaws found within these systems and how to better exploit them. This part of the course will also include web services and mobile applications due to their prevalence within modern organizations.

This information-packed advanced pen testing course will wrap up with a full-day Capture the Flag (CTF) event. This CTF event will target an imaginary organization's web applications and will include both Internet and intranet applications of various technologies. This event is designed to allow you to put the pieces together from the previous five days reinforcing the information and learning you will have gained.

The SANS promise is that you will be able to use these ideas immediately upon returning to the office in order to better perform penetration tests of your web applications and related infrastructure. This course will enhance your exploitation and defense skill sets as well as fulfill a need to teach more advanced techniques than can be covered in the foundational course, Security 542: Web Application Penetration Testing and Ethical Hacking.

**From the Author**

As web applications and their mobile counterparts become more complex and hardened against attack, penetration testers need to adjust the techniques they use to evaluate the security of these systems. This includes understanding how the various targets work, their usage of encryption and web application firewalls, and how to perform vulnerability discovery and exploitation against these items. This course is designed to expand past the methodology and focus on the how when we are presented with the challenges of web penetration testing.

-Kevin Johnson
<table>
<thead>
<tr>
<th>Existing Rule</th>
<th>Proposed Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1-Definitions</strong></td>
<td></td>
</tr>
<tr>
<td>1.1 &quot;District office of state concern&quot;</td>
<td>Definitions alphabetized, &quot;District Office of State Concern&quot; stricken; &quot;Score&quot; added, definitions amended and moved from 2(d), 2.20.1 a, 2.20.1 b, 2.20.1 d, 8.1.3, 8.1.1, 3.1, 8.1.2, 27.1.1, 27.1.2, 27.1.3, 27.1.4, 25.2.1, 42.2, 27.1.6, 42.10, 27.1.8, 21.1.7,</td>
</tr>
<tr>
<td><strong>2- Rules concerning Voter Registration</strong></td>
<td>2- Rules concerning voter registration</td>
</tr>
<tr>
<td>2.1 repealed</td>
<td>removed</td>
</tr>
<tr>
<td>2.2 fee for providing information</td>
<td>Amended and moved to 2.15.2</td>
</tr>
<tr>
<td>2.3 repealed</td>
<td>Removed</td>
</tr>
<tr>
<td>2.4 confidentiality of Agency in voter registration</td>
<td>Portions are included in 2.12</td>
</tr>
<tr>
<td>2.5 Confidentiality of voter information</td>
<td>Portions are included in 2.12</td>
</tr>
<tr>
<td>2.6 Information required from applicants for voter registration</td>
<td>???</td>
</tr>
<tr>
<td>2.7 Treatment of applications where the required information was not provided</td>
<td>Amended and moved to 2.4</td>
</tr>
<tr>
<td>2.8 Submission of voter registration forms</td>
<td>Amended and moved to 2.2</td>
</tr>
<tr>
<td>2.9 Registration of homeless voters</td>
<td>Amended and moved to 2.8</td>
</tr>
<tr>
<td>2.10 Changes to an electors voter registration record</td>
<td>Amended and moved to 2.5</td>
</tr>
<tr>
<td>2.11 Registration change must be provided to county clerk</td>
<td>Amended and moved to 2.6</td>
</tr>
<tr>
<td>2.12 Registration of Address Confidentiality Program (ACP) Electors</td>
<td>Portions included in new Rule 2.12</td>
</tr>
<tr>
<td>2.13 Preservation of Voter Registration Records</td>
<td>Amended and moved to 2.15.1</td>
</tr>
<tr>
<td>2.14 Effective date of voter registration application</td>
<td>Portions are included in 2.2.4</td>
</tr>
<tr>
<td>2.15 Repealed</td>
<td>Removed</td>
</tr>
<tr>
<td>2.16 Voter who believes his application was not correctly matched</td>
<td>Amended and moved to 2.10</td>
</tr>
<tr>
<td>2.17 Confirmation card if applicant is &quot;not registered&quot;</td>
<td>Amended and moved to 2.11</td>
</tr>
<tr>
<td>2.18 List Maintenance</td>
<td>Amended and moved to 2.13</td>
</tr>
<tr>
<td>2.19 Confirmation card</td>
<td>???</td>
</tr>
<tr>
<td>2.20. voter registration status designations</td>
<td>Amended and moved to 2.1</td>
</tr>
<tr>
<td>2.20.1 Definitions</td>
<td>Amended and moved to Rule 1.1.X</td>
</tr>
<tr>
<td>2.20.2 Effect of voter registration status designation</td>
<td>Amended and moved to Rule 2.1</td>
</tr>
<tr>
<td>2.21 Minimum matching criteria</td>
<td>Amended and moved to Rule 2.7</td>
</tr>
<tr>
<td>2.22 No consolidation or cancelation of duplicate records 90 days before a primary or general election</td>
<td>Amended and moved to 2.13</td>
</tr>
<tr>
<td>2.23 Repealed</td>
<td>Removed</td>
</tr>
<tr>
<td><strong>Rule 3-Rules concerning Qualified Political Organizations</strong></td>
<td>Rule 3- Rules concerning Qualified Political Organizations</td>
</tr>
<tr>
<td>3.1 Definitions of a qualified political organization</td>
<td>Moved to 1.1.</td>
</tr>
<tr>
<td>3.2 Required proof of an organization</td>
<td>Amended and moved to 3.1</td>
</tr>
<tr>
<td>3.3 Qualified Political Organizations shall meet once a year</td>
<td>Amended and moved to 3.2</td>
</tr>
<tr>
<td>Existing Rule</td>
<td>Proposed Rule</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>3.4 A qualified political organization shall place candidates on the general</td>
<td>Amended and moved to 3.3</td>
</tr>
<tr>
<td>election ballot every two years</td>
<td></td>
</tr>
<tr>
<td>3.5 A qualified political organization shall be qualified as soon as it:</td>
<td>Amended and moved to 3.4</td>
</tr>
<tr>
<td>3.6 Eligible electors shall be able to register as affiliated with political</td>
<td>Amended and moved to 3.5</td>
</tr>
<tr>
<td>organization</td>
<td></td>
</tr>
<tr>
<td>3.7 Political organizations shall lose status if they fail to do one of the</td>
<td>Amended and moved to 3.6</td>
</tr>
<tr>
<td>following</td>
<td></td>
</tr>
<tr>
<td>3.8 Secretary of State will notify Clerk and Recorder of lost status</td>
<td>Amended and moved to 3.7</td>
</tr>
<tr>
<td>3.9 Printouts and lists shall be supplied to organizations at the same rate</td>
<td>Amended and moved to 3.8</td>
</tr>
<tr>
<td>as charged for political parties</td>
<td></td>
</tr>
<tr>
<td>3.10 Summary reports of voter registration by political party</td>
<td>Amended and moved to 3.9</td>
</tr>
<tr>
<td>3.11 Electors must complete a Declaration of Party Affiliation when voting</td>
<td>Repealed</td>
</tr>
<tr>
<td>during a primary election</td>
<td></td>
</tr>
<tr>
<td>Rule 4- Rules concerning circulation of candidates petitions</td>
<td>Rule 4-Repealed</td>
</tr>
<tr>
<td>Rule 5- Rules concerning Non-Partisan Elections Not Coordinated by the County</td>
<td></td>
</tr>
<tr>
<td>Clerk</td>
<td></td>
</tr>
<tr>
<td>Rule 6- Rules concerning coordinated elections</td>
<td>Amended and moved to 4</td>
</tr>
<tr>
<td>6.1 Participation in coordinated election</td>
<td>Amended and moved to 4.1</td>
</tr>
<tr>
<td>6.2 Procedures for coordinated elections involving jurisdictions shared by</td>
<td>Amended and moved to 4.2</td>
</tr>
<tr>
<td>multiple counties</td>
<td></td>
</tr>
<tr>
<td>6.3 Form of election for November coordinated elections</td>
<td>Amended and moved to 4.3</td>
</tr>
<tr>
<td>6.4 Form of coordinated elections held other than in November</td>
<td>Amended and moved to 4.4</td>
</tr>
<tr>
<td>6.5 Determinations of Ballot issues and texts</td>
<td>Amended and moved to 4.5</td>
</tr>
<tr>
<td>6.6 Colo. Const. Art. X Sec. 20 notice requirements</td>
<td>Amended and moved to 4.9</td>
</tr>
<tr>
<td>6.7 Written comments concerning ballot issues</td>
<td>Amended and moved to 4.9.7</td>
</tr>
<tr>
<td>Rule 7- Rules concerning Polling Places</td>
<td>Rule 7- Rules concerning elections conducted by the</td>
</tr>
<tr>
<td>7.1 polling place materials</td>
<td>county clerk</td>
</tr>
<tr>
<td>7.2 Coordinated elections do not have to be in political subdivision</td>
<td>Portions are included in 7.7</td>
</tr>
<tr>
<td>7.3 Polling places for partisan elections</td>
<td>Repealed</td>
</tr>
<tr>
<td>7.4 Polling place notice</td>
<td>Repealed</td>
</tr>
<tr>
<td>7.5 voter center guidelines</td>
<td>Repealed</td>
</tr>
<tr>
<td>7.6 Time in voting area</td>
<td>Portions are included in 7.7</td>
</tr>
<tr>
<td>7.7 Polling place accessibility</td>
<td>Portions are included in 7.8, 12.1</td>
</tr>
<tr>
<td>Rule 8- Rules concerning watchers</td>
<td>Rule 8- Rules concerning watchers</td>
</tr>
<tr>
<td>Existing Rule</td>
<td>Proposed Rule</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>8.1- Definitions</td>
<td>Moved to 1.1</td>
</tr>
<tr>
<td>8.2- Qualifications of watchers</td>
<td>Amended and moved to 8.1</td>
</tr>
<tr>
<td>8.3- Political party attorneys not allowed in polling place</td>
<td>Amended and moved to 8.2</td>
</tr>
<tr>
<td>8.4 Watchers are not permitted to have</td>
<td>Amended and moved to 8.3</td>
</tr>
<tr>
<td>8.5- List of eligible electors</td>
<td>Amended and moved to 8.4</td>
</tr>
<tr>
<td>8.6 -Watchers are subject to 1-5-503</td>
<td>Portions amended and moved to 1.1, 8.5</td>
</tr>
<tr>
<td>8.7 What watchers may observe</td>
<td>Amended and moved to 8.6</td>
</tr>
<tr>
<td>8.8- Limitations of watchers</td>
<td>Amended and moved to 8.7</td>
</tr>
<tr>
<td>8.9-Appointment of watchers</td>
<td>Amended and moved to 8.8</td>
</tr>
<tr>
<td>8.10 - Observers appointed by Federal Government</td>
<td>Amended and moved to 8.9</td>
</tr>
<tr>
<td>8.11- Watchers and observers at recount</td>
<td>Amended and moved to 8.10</td>
</tr>
<tr>
<td>8.12- Media observers</td>
<td>Amended and moved to 8.11</td>
</tr>
<tr>
<td>8.13- watchers at vote centers</td>
<td>Amended and moved to 8.12</td>
</tr>
<tr>
<td>8.14- Election official shall certify all watchers</td>
<td>Amended and moved to 8.13</td>
</tr>
<tr>
<td>8.15- Removal of watchers</td>
<td>Amended and moved to 8.14</td>
</tr>
<tr>
<td>8.16 -Only one watcher per polling place</td>
<td>Amended and moved to 8.15</td>
</tr>
<tr>
<td>8.17- Watchers may be appointed to observe recalls</td>
<td>Amended and stays at 8.17</td>
</tr>
<tr>
<td><strong>Rule 9- Rules concerning voting assistance for voters with disabilities.</strong></td>
<td>Relocated to Rule 7</td>
</tr>
<tr>
<td>9.1- The county clerk and recorder must post a sign</td>
<td>Moved to rule 7.10</td>
</tr>
<tr>
<td>9.2-when a voter spoils 2 ballots an election judge shall offer assistance</td>
<td>Amended and moved to 7.10</td>
</tr>
<tr>
<td><strong>Rule 10-Rules concerning Ballots and Election Supplies-</strong></td>
<td>Amended and moved to 4</td>
</tr>
<tr>
<td>10.1 Text of ballot questions should be printed in certain ways</td>
<td>Amended and moved to 4.8.1</td>
</tr>
<tr>
<td>10.2 If the ballot is printed in error- the ballot should be corrected according to the Secretary of State.</td>
<td>Amended and moved to 4.8.5</td>
</tr>
<tr>
<td>10.3 If no candidate</td>
<td>Amended and moved to 4.8.2</td>
</tr>
<tr>
<td>10.4 candidates listed on the ballot must provide an audio recording of pronunciation of name</td>
<td>Amended and consolidated into 4.6.1</td>
</tr>
<tr>
<td>10.5 County candidates must also provide an audio with the pronunciation of their names</td>
<td>Amended and consolidated into 4.6.2</td>
</tr>
<tr>
<td><strong>Rule 11- Rules concerning voting systems</strong></td>
<td><strong>Rule 11- Rules concerning voting systems</strong></td>
</tr>
<tr>
<td>11.1 Definitions-</td>
<td>New definitions added and one definition repealed, the rest amended</td>
</tr>
<tr>
<td>11.2 Voting System Access</td>
<td>Amended and stays at 11.2</td>
</tr>
<tr>
<td>11.3 Performance Bond</td>
<td>Amended and stays at 11.3</td>
</tr>
<tr>
<td>11.4 Voting systems inventory</td>
<td>Amended and stays at 11.4</td>
</tr>
<tr>
<td>11.5 Voting systems testing</td>
<td>Amended and sections within 11.5 are completely renumbered, stays at 11.5</td>
</tr>
<tr>
<td>11.6 Procedures for Voter-Verifiable Paper Audit Trail</td>
<td>Moved to 43.2.10</td>
</tr>
<tr>
<td>Existing Rule</td>
<td>Proposed Rule</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Escrow of County Election Set Up</td>
<td>Amended and moved to 11.6</td>
</tr>
<tr>
<td>Escrow of voting system software</td>
<td>Amended and moved to 45.12</td>
</tr>
</tbody>
</table>

**Rule 12- Rules concerning mail ballot elections**

<table>
<thead>
<tr>
<th>Existing Rule</th>
<th>Proposed Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1- Definitions</td>
<td>Moved to rule 1</td>
</tr>
<tr>
<td>12.2- Election Judges</td>
<td>??</td>
</tr>
<tr>
<td>12.3- Notice of Elections</td>
<td>Amended and moved to 5.1</td>
</tr>
<tr>
<td>12.4- Mail ballot plans</td>
<td>Amended and moved to 7.1</td>
</tr>
<tr>
<td>12.5- Ballots</td>
<td>Amended and moved to 7.2</td>
</tr>
<tr>
<td>12.6- Mail-in and Early voting</td>
<td>Repealed</td>
</tr>
<tr>
<td>12.7- Receipt of Ballots</td>
<td>Amended and moved to 5.2.4</td>
</tr>
<tr>
<td>12.8- Voter directed to return form with ballot</td>
<td>Repealed</td>
</tr>
<tr>
<td>12.9- Signature verification</td>
<td>Portions included in new Rule 7.6</td>
</tr>
<tr>
<td>12.10- Ballots delivered in person</td>
<td>Amended and moved to 7.5</td>
</tr>
<tr>
<td>12.11- Request for a replacement ballot</td>
<td>??</td>
</tr>
<tr>
<td>12.12- Surrender of mail ballot</td>
<td>Portions included in 7.7.5</td>
</tr>
<tr>
<td>12.13- Judges Duties</td>
<td>??</td>
</tr>
<tr>
<td>12.14- Canvass of votes/certificates of election</td>
<td>??</td>
</tr>
</tbody>
</table>

**Rule 13- Rules concerning mail-in voting**

<table>
<thead>
<tr>
<th>Existing Rule</th>
<th>Proposed Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1- All materials may be included in ballot packet</td>
<td>Moved to 5.2.3</td>
</tr>
<tr>
<td>13.2- Keep track of people who deliver more than 10 mail ballots</td>
<td>Amend and moved to 7.5</td>
</tr>
<tr>
<td>13.3- County clerk and recorder shall notify all the people from 13.2 that they have broken the law</td>
<td>Amend and moved to 7.5</td>
</tr>
<tr>
<td>13.4- Submit a picture ID with return ballot</td>
<td>??</td>
</tr>
<tr>
<td>13.5- The county clerk shall show which voters need to return ID with the ballot</td>
<td>??</td>
</tr>
<tr>
<td>13.6- Must return all pages of the multi-page ballot</td>
<td>??</td>
</tr>
<tr>
<td>13.7- If required to return ID, outside of envelope should be marked to show this</td>
<td>??</td>
</tr>
<tr>
<td>13.8- If envelop marked for ID, but no ID is sent</td>
<td>??</td>
</tr>
<tr>
<td>13.9- What election judge should open if a form is required with the ballot</td>
<td>??</td>
</tr>
<tr>
<td>13.10- For nonmatching or missing signatures</td>
<td>??</td>
</tr>
<tr>
<td>13.11- Election officials duties are triggered under 1-8-112 if-</td>
<td>??</td>
</tr>
<tr>
<td>13.12- Mail in voters who come to the polling place</td>
<td>??</td>
</tr>
<tr>
<td>13.13- Permanent Mail in voting</td>
<td>??</td>
</tr>
<tr>
<td>13.14- Using the Ballot Now system, clerk must create ballots 32 days before election</td>
<td>??</td>
</tr>
<tr>
<td>13.15- County clerk is in possession of ballots once vendor has prepared ballots for mailing</td>
<td>??</td>
</tr>
<tr>
<td>13.16- Secrecy sleeve should say:</td>
<td>??</td>
</tr>
<tr>
<td>13.17- Voter signature on the back of the envelope should be concealed</td>
<td>??</td>
</tr>
<tr>
<td>13.18- A properly executed mail in ballot may be submitted</td>
<td>??</td>
</tr>
<tr>
<td>Existing Rule</td>
<td>Proposed Rule</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>13.19- Cannot issue a mail in ballot to an inactive voter</td>
<td>???</td>
</tr>
<tr>
<td>13.20- An overseas votes whose record is inactive may:</td>
<td>Amended moved to 16</td>
</tr>
<tr>
<td><strong>Rule 14- Rules concerning recount</strong></td>
<td>Amended and moved to 10</td>
</tr>
<tr>
<td>15.1 License, Registration and filing procedures</td>
<td>Amended and stays at 15.1</td>
</tr>
<tr>
<td>15.2-Petition representatives</td>
<td>Amended and stays at 15.2</td>
</tr>
<tr>
<td>15.3- Petition circulation</td>
<td>Amended and stays at 15.3</td>
</tr>
<tr>
<td>15.4- Only one filing of a petition or an addendum</td>
<td>Amended and stays at 15.4</td>
</tr>
<tr>
<td>15.5- Verification by random sample</td>
<td>Amended and stays at 15.4</td>
</tr>
<tr>
<td><strong>Rule 16- Repealed</strong></td>
<td>Repealed</td>
</tr>
<tr>
<td><strong>Rule 17 - General Rules Concerning Verification of Petitions</strong></td>
<td>Amended and moved to 15</td>
</tr>
<tr>
<td>17.1- General procedures concerning verification procedure</td>
<td>Amended and moved to 15.5</td>
</tr>
<tr>
<td>17.2- Checking the circulators affidavit</td>
<td>Amended and moved to 15.6</td>
</tr>
<tr>
<td>17.3- Checking individual's signature</td>
<td>Amended and moved to 15.8</td>
</tr>
<tr>
<td>17.4- Final Tally</td>
<td>Repealed</td>
</tr>
<tr>
<td><strong>Rule 18- Rules Concerning Statement of Sufficiency for Petitions</strong></td>
<td>Repealed</td>
</tr>
<tr>
<td><strong>Rule 19- Rules Concerning Cure for Statewide Petitions</strong></td>
<td>Amended and moved to 15</td>
</tr>
<tr>
<td>19.1-Cure of Petitions deemed insufficient</td>
<td>Amended and moved to 15.9</td>
</tr>
<tr>
<td>19.2-If proponents submit additional signatures</td>
<td>Amended and moved to 15.9</td>
</tr>
<tr>
<td>19.3- 110% shall be sufficient</td>
<td>Amended and moved to 15.9</td>
</tr>
<tr>
<td>19.4 - In between 110% and 90% - all submissions will be checked</td>
<td>Amended and moved to 15.9</td>
</tr>
<tr>
<td>19.5- If initial check was of every entry</td>
<td>Amended and moved to 15.9</td>
</tr>
<tr>
<td>19.6- Designated election official shall issue a new certificate</td>
<td>???</td>
</tr>
<tr>
<td><strong>Rule 20- Rules Concerning Protests</strong></td>
<td>Amended and moved to 15</td>
</tr>
<tr>
<td>20.1- A protests shall specifically state the reasons for the challenge</td>
<td>Amended and moved to 15.10</td>
</tr>
<tr>
<td>20.2- Individual entry must be listed</td>
<td>Amended and moved to 15.10</td>
</tr>
<tr>
<td>20.3- When random sample is protested</td>
<td>Amended and moved to 15.10</td>
</tr>
<tr>
<td>20.4- Individual entries not checked cannot be protested</td>
<td>Amended and moved to 15.10</td>
</tr>
<tr>
<td><strong>Rule 21- Rules concerning ballot issue elections</strong></td>
<td>Amended and moved to Rule 4</td>
</tr>
<tr>
<td>21.1 Placing measures on the ballot for coordinated odd year elections</td>
<td>Amended and moved to 4</td>
</tr>
<tr>
<td>21.2-written comments concerning ballot issues</td>
<td>Amended and moved to 4</td>
</tr>
<tr>
<td><strong>Rule 22</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Rule 23- Rules concerning referendum petitions</strong></td>
<td>Amended and moved to rule 15.11</td>
</tr>
<tr>
<td>23.1-Applicability</td>
<td>Amended and Moved to 15.11.1</td>
</tr>
<tr>
<td>Existing Rule</td>
<td>Proposed Rule</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>23.2- Relationship to statutory and constitutional provisions</td>
<td>Deleted</td>
</tr>
<tr>
<td>23.3- Applicability of initiative statutes</td>
<td>Amended and Moved to 15.11.2 and 15.11.3</td>
</tr>
<tr>
<td>23.4- Approval of referendum petition form</td>
<td>Amended and moved to 15.11.4, 15.11.5</td>
</tr>
<tr>
<td>23.5- Ballot Title and submission clause</td>
<td>Amended and moved to 15.11.7, 15.11.8</td>
</tr>
<tr>
<td>23.6- Election</td>
<td>Amended and moved to 15.11.9</td>
</tr>
<tr>
<td><strong>Rule 24- Rules concerning congressional term limits declaration</strong></td>
<td></td>
</tr>
<tr>
<td>24.1- Congressional term limits declaration will be made available to all congressional candidates</td>
<td>Amended and moved to Rule 4.7</td>
</tr>
<tr>
<td>24.2- Part A shall be accepted by Sec of State</td>
<td>Amended and moved to 4.7.1</td>
</tr>
<tr>
<td>24.3- In case a candidate has qualified for a term that would exceed term limits</td>
<td>Amended and moved to 4.7.2</td>
</tr>
<tr>
<td><strong>Rule 25- Rules Concerning UOCAVA</strong></td>
<td></td>
</tr>
<tr>
<td>25.1 General rules covering UOCAVA</td>
<td>Moved to 16</td>
</tr>
<tr>
<td>25.2 Electronic Ballot Transmission</td>
<td>Portions are amended and stay at 25.2, portions are moved to rule 1</td>
</tr>
<tr>
<td><strong>Rule 26- Rules Concerning Provisional Voting</strong></td>
<td>Moved to 17</td>
</tr>
<tr>
<td><strong>Rule 27- Rules Concerning Uniform Ballot Counting Standards</strong></td>
<td>Moved to 18</td>
</tr>
<tr>
<td>Rule 28</td>
<td>Moved to 6</td>
</tr>
<tr>
<td>Rule 29</td>
<td>Amended and moved to 7.6</td>
</tr>
<tr>
<td>Rule 30-</td>
<td>Repealed - portions incorporated into Rule 2</td>
</tr>
<tr>
<td>Rule 31-</td>
<td>Amended and moved to 13</td>
</tr>
<tr>
<td>Rule 32-</td>
<td>Moved to Rule 12</td>
</tr>
<tr>
<td>Rule 33</td>
<td>Amended and moved to 7.7.7</td>
</tr>
<tr>
<td>Rule 34</td>
<td>Amended and moved to 11.9</td>
</tr>
<tr>
<td>Rule 35</td>
<td>Amended and moved to 11.12</td>
</tr>
<tr>
<td>Rule 36</td>
<td>Amended and moved to 11.10</td>
</tr>
<tr>
<td>Rule 37</td>
<td>Repealed - portions incorporated into 11</td>
</tr>
<tr>
<td>Rule 38</td>
<td>Amended and moved to 43</td>
</tr>
<tr>
<td>Rule 39</td>
<td>Repealed - portions incorporated into 2</td>
</tr>
<tr>
<td><strong>Rule 40- Rules concerning canvassing</strong></td>
<td></td>
</tr>
<tr>
<td>41.1-Definitions</td>
<td>Amended and moved to Rule 10</td>
</tr>
<tr>
<td>41.2- Appointment to the Canvass Board</td>
<td></td>
</tr>
<tr>
<td>41.3- Duties of the canvass board</td>
<td></td>
</tr>
<tr>
<td>41.4- Detailed Ballot Log</td>
<td></td>
</tr>
<tr>
<td>41.5- Election day tracking process</td>
<td></td>
</tr>
<tr>
<td>41.6- Designated election officials disposition of forms</td>
<td></td>
</tr>
<tr>
<td>41.7- Procedures for the day of canvass</td>
<td></td>
</tr>
<tr>
<td>41.8- Official abstract</td>
<td></td>
</tr>
<tr>
<td>41.9- The abstract is Official permanent record</td>
<td></td>
</tr>
<tr>
<td>41.10- Appointment of canvass workers</td>
<td></td>
</tr>
<tr>
<td>41.11-Voter History</td>
<td></td>
</tr>
<tr>
<td>41.12- Written complaints</td>
<td></td>
</tr>
<tr>
<td>41.13- Role of watchers</td>
<td></td>
</tr>
<tr>
<td>41.14- Role of Sec of State</td>
<td></td>
</tr>
<tr>
<td>Existing Rule</td>
<td></td>
</tr>
<tr>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>Rule 42</td>
<td></td>
</tr>
<tr>
<td>Rule 43</td>
<td></td>
</tr>
<tr>
<td>43.1 - Definitions</td>
<td>Amended and stays at 43.1</td>
</tr>
<tr>
<td>43.2 - Annual security plan</td>
<td>Amended and stays at 43.2</td>
</tr>
<tr>
<td>43.3 -</td>
<td></td>
</tr>
<tr>
<td>43.4 - Amendments and review of security plans</td>
<td>Amended and moved to 43.3</td>
</tr>
<tr>
<td>43.5 - Lease, loan, or rental of election equipment</td>
<td>Amended and moved to 43.4</td>
</tr>
<tr>
<td>Rule 44</td>
<td></td>
</tr>
<tr>
<td>44.1 - Statement of Intent</td>
<td>Amended and moved to 14</td>
</tr>
<tr>
<td>44.2 - Training</td>
<td>Amended and moved to 14.2</td>
</tr>
<tr>
<td>44.3 - Number Assigned</td>
<td>Amended and moved to 14.3</td>
</tr>
<tr>
<td>44.4 - VRD Voter Application Forms</td>
<td>Amended and moved to 14.4</td>
</tr>
<tr>
<td>44.4.4</td>
<td></td>
</tr>
<tr>
<td>44.6 - VRD Complaints and Fines</td>
<td>Amended and moved to 14.5</td>
</tr>
<tr>
<td>Rule 45</td>
<td></td>
</tr>
<tr>
<td>45.12 - Purchases and Contracts</td>
<td>Amended and moved to 11.11</td>
</tr>
<tr>
<td>Rule 46 - Repealed</td>
<td></td>
</tr>
<tr>
<td>Rule 47</td>
<td></td>
</tr>
<tr>
<td>Rule 48</td>
<td></td>
</tr>
<tr>
<td>Rule 49</td>
<td></td>
</tr>
<tr>
<td>49.1 - SCORE username and password administration</td>
<td>Amended and moved to 2.16</td>
</tr>
<tr>
<td>49.2 - Custodianship of Voter Registration Information</td>
<td>Amended and moved to 2.15.4</td>
</tr>
<tr>
<td>Rule 50</td>
<td></td>
</tr>
<tr>
<td>Rule 51</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Amended and stays</td>
</tr>
</tbody>
</table>
Disclaimer:
This is a proposed recodification of the Colorado Election Rules. Current 8 CCR 1505-1, is stricken in its entirety and re-codified as follows. Some current rule language is retained either in full or as amended.

This is a working draft of the recodification. Please note that there may be technical errors, such as incorrect or missing citations. But we are involving you at this early stage because the Secretary values your feedback.

Please send your feedback by August 7, 2013. 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:

<table>
<thead>
<tr>
<th>Font effect</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sentence case</td>
<td>Retained/modified current rule language</td>
</tr>
<tr>
<td>SMALL CAPS</td>
<td>New language</td>
</tr>
<tr>
<td>Strikethrough</td>
<td>Deletions</td>
</tr>
<tr>
<td>[Italic blue font text]</td>
<td>Annotations</td>
</tr>
</tbody>
</table>

[Current 8 CCR 1505-1 is stricken in its entirety and re-codified as follows:]

Rule 1. Definitions

1.1 As used in these Rules and the “Uniform Election Code of 1992” unless the context otherwise requires, the following terms shall have the meanings indicated:

“District office of state concern” means any of the following offices: Member of the State Board of Education, Member of the Board of Regents of the University of Colorado, and Member of the Board of Directors of the Regional Transportation District.

As used in these Rules, unless stated otherwise:

1.1.1 “ACTIVE STATUS” OR “ACTIVE RECORD” MEANS THAT THERE ARE NO CONDITIONS OR RESTRICTIONS ON THE ELECTOR’S ELIGIBILITY OR REGISTRATION RECORD.

[Relocated from 2.20.1 a., with amendments]
1.1.2 “Ballot measure” means a ballot issue or ballot question as defined in sections 1-1-104(2.3) and (2.7), C.R.S.

[Relocated from 27.1.1., with amendments]

1.1.3 “Blank ballot” means a ballot on which the voter has made no marks in any voting position, has marked with an unreadable marker, or has consistently marked outside of the “read” area of the scanner.

[Relocated from 27.1.2., with amendments]

1.1.4 “Cancelled status” or “cancelled record” means that the county clerk and recorder cancelled the elector’s voter registration record because the elector:

(A) Is not eligible to vote;

(B) Is not registered to vote; or

(C) Has withdrawn his or her registration.

[Relocated from 2.20.1 b., with amendments]

1.1.5 “Canvass board” means a committee composed of the county clerk and recorder and the registered electors appointed by the major parties in accordance with section 1-10-101, C.R.S.

[Relocated from 41.1.1]

1.1.6 “Canvass workers” means workers appointed or hired by the designated election official to assist in the preparation and conduct of the canvass.

[Relocated from 41.1.2]

1.1.7 “Central count” means a ballot counting process in which the county clerk and recorder tabulates cumulative voting totals for multiple precincts and ballot styles at a single location.

[Relocated from 11.1.1., with amendments]

1.1.8 “Damaged ballot” means a ballot that is torn, bent, or otherwise mutilated or rendered unreadable, so that it cannot be processed by the optical scanner ballot reader.

(A) Damaged ballots include all ballots that contain a foreign substance that could interfere with the optical scan machine (i.e. food, drink, etc.).

(B) Damaged ballots may include ballots that are marked in a
MEDIUM OTHER THAN THE MEDIUM INDICATED IN THE BALLOT INSTRUCTIONS.

[Relocated from 27.1.3., with amendments]

1.1.9 “DATA ENTRY COUNTY” MEANS A COUNTY USING AN ELECTION MANAGEMENT SYSTEM THAT EXPORTS A FILE TO BE DIRECTLY UPLOADED TO THE ELECTION NIGHT RESULTS SYSTEM.

1.1.10 “DESIGNATED ELECTION OFFICIAL,” AS USED IN RULE 11, INCLUDES THE DESIGNATED ELECTION OFFICIAL’S SWORN, DEPUTIZED DESIGNEE.

1.1.11 “DUPLICATED BALLOT” MEANS A BALLOT FOR WHICH A TRUE COPY MUST BE MADE FOR THE BALLOT TO BE PROPERLY PROCESSED AND COUNTED BECAUSE OF DAMAGE, IMPROPER MARKING OR ANY ISSUE THAT WOULD PREVENT A BALLOT TABULATING MACHINE FROM ACCURATELY COUNTING THE BALLOT.

[Relocated from 27.1.4., with amendments]

1.1.12 “ELECTION COMPLAINT” MEANS A COMPLAINT FILED WITH THE SECRETARY OF STATE UNDER TITLE 1, C.R.S.

1.1.13 “ELECTION SETUP RECORDS” MEANS THE ELECTRONIC RECORDS, OFTEN IN THE FORM OF A DATABASE OR A SET OF DATABASES, GENERATED BY ELECTION TABULATION SOFTWARE TO CREATE AND DEFINE BALLOTS, TABULATION INSTRUCTION, AND OTHER FUNCTIONS RELATED TO THE ELECTION.

[Relocated from 11.1.2., with amendments]

1.1.14 “ELECTION SOFTWARE” MEANS THE SOFTWARE FOR ELECTION EQUIPMENT OR COMPUTERS THAT CONTROLS ELECTION SETUP VOTE RECORDING, VOTE TABULATION, AND REPORTING.

[Relocated from 11.1.4., with amendments]

1.1.15 “ELECTRONIC BALLOT” MEANS A NON-PAPER BALLOT SUCH AS ON A TOUCH SCREEN OR THROUGH AUDIO FEEDBACK. AFTER A VOTER CASTS AN ELECTRONIC BALLOT, THE VOTER’S CHOICES MUST BE:

(A) MARKED AND PRINTED ON A PAPER BALLOT FOR SUBSEQUENT COUNTING BY A PAPER BALLOT SCANNING DEVICE; OR

(B) DIGITALLY RECORDED AND COUNTED BY THE TOUCH SCREEN DEVICE, COMMONLY REFERRED TO AS A DIRECT RECORDING ELECTRONIC (DRE) DEVICE.

[Relocated from 11.1.6., with amendments]
“Electronic Transmission” means:

(A) For the purpose of sending an unvoted ballot to the elector fax, email, and online ballot delivery.

(B) For the purpose of returning a voted ballot to the county clerk and recorder fax and email.

[Relocated from 25.2.1 and 42.2, with amendments]

“Electronic Voting Device” means a device by which votes are recorded electronically, including a touch screen system.

[Relocated from 11.1.7., with amendments]

“Firmware” means computer programs, stored on read-only memory devices or other electronic circuitry in voting devices, that control the basic operation and function of those devices.

[Relocated from 11.1.8., with amendments]

“Help America Vote Act complaint” or “HAVA complaint” means a complaint filed with the Secretary of State under Title III of the Help America Vote Act (HAVA) and Article 1.5 of Title 1, C.R.S.

“Immediate Voting Area” means the area that is within six feet of the voting equipment, voting booths, and the ballot box.

[Relocated from 8.6.1., with amendments]

“Inactive Status” means a restriction a county clerk and recorder places on an elector’s record if the United States Postal Service returns a mail ballot, voter information card, or confirmation card to the county clerk and recorder as undeliverable.

[Relocated from 2.20.1 d., with amendments]

“Logic and Accuracy Test” or “LAT” means a step-by-step documented review of a voting device’s ability, prior to use in any election, to accurately produce voter choices for the candidates and ballot measures in an election. The Logic and Accuracy Test must fulfill the requirements of the public test described in section 1-7-509 (2), C.R.S.

[Relocated from 11.1.9., with amendments]

“Manual Entry County” means a county that does not use an election management system to export data.
1.1.24 "MEDIA OBSERVER" MEANS AN OBSERVER WITH VALID AND CURRENT MEDIA
CREDENTIALS.

[Relocated from 8.1.3., with amendments]

1.1.25 "OFFICIAL OBSERVER" MEANS EITHER AN OBSERVER APPOINTED BY THE
SECRETARY OF STATE OR AN OBSERVER APPOINTED BY THE FEDERAL GOVERNMENT
AND APPROVED BY THE SECRETARY OF STATE. OFFICIAL OBSERVERS MAY BE
PRESENT IN ALL PHASES OF THE ELECTION PROCESS, BUT ARE SUBJECT TO RULES
AND REGULATIONS AS PRESCRIBED BY THE SECRETARY OF STATE AND PERFORM
DUTIES AS MAY BE ASSIGNED BY THE SECRETARY OF STATE.

[Relocated from 8.1.1.]

1.1.26 "OVERVOTE" MEANS A RACE OR BALLOT MEASURE WHERE THE VOTER MARKED
VOTES FOR MORE THAN THE MAXIMUM NUMBER OF CANDIDATES OR RESPONSES FOR
A BALLOT MEASURE ALLOWED.

[Relocated from 27.1.6., with amendments]

1.1.27 "QUALIFIED POLITICAL ORGANIZATION" MEANS AN ORGANIZATION THAT HAS
PLACED A CANDIDATE FOR CONGRESSIONAL OR STATE OFFICE ON THE BALLOT IN A
CONGRESSIONAL VACANCY OR GENERAL ELECTION, WHOSE OFFICERS HAVE FILED
PROOF OF ORGANIZATION WITH THE SECRETARY OF STATE, AND THAT CONTINUES
to meet the requirements of Rules 3.3 and 3.4. [BAER v. MEYER, 728 F.2d 47
(10TH CIR. 1984)]

[Relocated from 3.1, with amendments]

1.1.28 "RELATED TO THE SECOND DEGREE" MEANS SPOUSE, CIVIL UNION PARTNER,
PARENTS, CHILDREN, BROTHERS AND SISTERS, GRANDPARENTS, AND
GRANDCHILDREN RELATED BY BLOOD OR MARRIAGE.

[Relocated from 42.10, with amendments]

1.1.29 "SCORE" MEANS THE CENTRALIZED STATEWIDE REGISTRATION SYSTEM AND THE
COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST DESCRIBED IN PART 3 OF
ARTICLE 2 OF TITLE 1.

1.1.30 "Statement of Ballots Form" means the form used at the polling location that
accounts for all ballots at that location and includes all information required by
this rule.

[Relocated from 41.1.3]

1.1.31 "TARGET AREA" MEANS:

(A) THE SQUARE OR OVAL OPPOSITE THE CANDIDATE’S NAME OR BALLOT
RESPONSE ON A PAPER BALLOT; OR

(B) THE OVAL, INCOMPLETE LINE, OR INCOMPLETE ARROW OPPOSITE THE CANDIDATE’S NAME OR BALLOT RESPONSE (EXAMPLES: “Yes”, “No”, “For” or “Against”) ON AN OPTICAL SCAN BALLOT.

[Relocated from 27.1.8, with amendments]

1.1.32 “UNDERVOTE” MEANS A RACE OR BALLOT MEASURE WHERE THE VOTER MARKED VOTES FOR FEWER THAN THE MAXIMUM NUMBER OF CANDIDATES OR RESPONSES FOR A BALLOT MEASURE ALLOWED.

[Relocated from 27.1.7, with amendments]

1.1.33 “VOTING SYSTEM” AS DEFINED IN 1-1-104(50.8), C.R.S., DOES NOT INCLUDE VOTER REGISTRATION APPLICATIONS OR SYSTEMS, ELECTRONIC POLLBOOKS, BALLOT DELIVERY AND RETRIEVAL SYSTEMS, SIGNATURE VERIFICATION AND BALLOT SORTING DEVICES, BALLOT ON DEMAND PRINTERS, ELECTION NIGHT REPORTING AND OTHER ELECTION REPORTING SYSTEMS, AND OTHER COMPONENTS USED THROUGHOUT THE ELECTION PROCESS THAT DO NOT CAPTURE AND TABULATE VOTES.

1.1.34 “VVPAT” HAS THE SAME MEANING AS IN SECTION 1-1-104(50.6), C.R.S.

[Relocated from 11.1.12., with amendments]

1.1.35 “WATCHER” MEANS AN ELIGIBLE ELECTOR, OTHER THAN A CANDIDATE ON THE BALLOT, SELECTED BY A POLITICAL PARTY CHAIRPERSON ON BEHALF OF THE POLITICAL PARTY, BY A PARTY CANDIDATE AT A PRIMARY OR RECALL ELECTION, BY AN UNAFFILIATED CANDIDATE AT A GENERAL, CONGRESSIONAL VACANCY, NONPARTISAN, OR RECALL ELECTION, OR BY A PERSON DESIGNATED BY EITHER THE OPPONENTS OR PROPONENTS IN THE CASE OF A BALLOT ISSUE OR BALLOT QUESTION. IF SELECTED BY A POLITICAL PARTY CHAIRPERSON, A PARTY CANDIDATE, OR AN UNAFFILIATED CANDIDATE, THE WATCHER MUST BE AFFILIATED WITH THAT POLITICAL PARTY OR UNAFFILIATED AS SHOWN ON THE REGISTRATION BOOKS OF THE COUNTY CLERK AND RECORDER. A DESIGNATED WATCHER NEED NOT BE A RESIDENT OF THE COUNTY HE OR SHE IS DESIGNATED IN AS LONG AS HE OR SHE IS AN ELIGIBLE ELECTOR IN THE STATE OF COLORADO. [SECTION 1-1-104(51), C.R.S.]

[Relocated from 8.1.2, with amendments]

1.1.36 “WRITE-IN VOTE” MEANS A VOTE WHERE THE VOTER PHYSICALLY WRITES IN THE NAME OF A LEGALLY QUALIFIED WRITE-IN CANDIDATE IN THE SPACE RESERVED ON THE BALLOT FOR WRITE-IN VOTES AND PROPERLY MARKS THE TARGET AREA ACCORDING TO VOTER INSTRUCTIONS.

1.1.37 “ZERO TAPE” MEANS A PRINTOUT OF THE INTERNAL DATA REGISTERS IN ELECTRONIC VOTE-TABULATING EQUIPMENT INDICATING A VALUE OF ZERO.
Rule 2. Rules Concerning Voter Registration

2.20.2-2.1 Effect of voter registration status designation

a. 2.1.1 A COUNTY CLERK AND RECORDER MUST LIST THE NAME OF EVERY active status or active record voters’ ELECTOR names will appear on in the poll book, POLLBOOK, they will be sent a ballot in AND SEND HIM OR HER a mail ballot election, and they will be sent election NOTICES. notice mailings.

b. 2.1.2 A COUNTY CLERK AND RECORDER MUST ENSURE THAT THE NAME OF EVERY cancelled status or cancelled record voters’ records will remain ELECTOR APPEARS in the statewide voter registration database however, SCORE BUT their names will not appear on the poll book—POLLBOOK. They—THE COUNTY CLERK AND RECORDER will MAY not send a MAIL ballot in a mail ballot election, and they will not be sent OR election notice mailings NOTICES TO CANCELLED ELECTORS.

e. 2.1.3 Inactive—failed to vote status voters’ STATUS ELECTORS are eligible voters their ELECTORS WHOSE names will appear on the poll book and they will be sent election notice mailings—but THE COUNTY CLERK AND RECORDER MAY NOT SEND A MAIL BALLOT TO INACTIVE ELECTORS. Inactive—failed to vote voters will be sent a ballot in a mail ballot election where specifically required by sections 1-7.5-107 and 1-7.5-108.5(b), C.R.S.

d. Inactive—returned mail status or inactive—undeliverable status voters are eligible voters and their names will appear on the poll book. However, they will not be sent ballots in a mail ballot election and they will not be sent election notice mailings.

e. Inactive—undeliverable ballot status voters are eligible voters and their names will appear on the poll book. However, they will not be sent a ballot in a mail ballot election and they will not be sent election notice mailings.

2.8-2.2 Submission of voter registration forms

2.2.1 An applicant may submit a properly executed voter registration form may be submitted to the county clerk and recorder in person, by mail, by fax, by online voter registration, or as a scanned AN EMAIL attachment. to an email.

2.8.1-2.2.2 All voter registrations APPLICATIONS submitted by mail, fax, or as a PDF AN EMAIL attachment to an email shall be treated as—ARE mail registrations.

[Section 1-2-501, C.R.S., Election Rule 30.3]
2.8.2.2.3 If any portion of a MAIL APPLICATION voter registration submitted by "mail" is illegible, the county clerk and recorder shall MUST notify the applicant of the additional information required in accordance with section 1-2-509, C.R.S.

2.8.2.2.4 For the purpose of submitting voter registration applications by fax, email or online voter registration, close of business shall be 11:59pm MT.

2.2.5 Under section 1-5-509, C.R.S., the effective date of a voter registration application received by the secretary of state is the earlier of the date the application is received or the date of the legible postmark.

2.2.6 If a county clerk and recorder receives a paper voter registration application between 21 and 7 days before election day, the county clerk must send the applicant notification by regular mail, or email if provided, within one business day after receiving the application that the applicant is registered to vote but will not receive a ballot by mail. The notice must state that, if the applicant wishes to vote in the upcoming election, the applicant must either register online via the online voter registration system or in person at the county clerk and recorder’s office or at a voter service and polling center, whichever is applicable.

2.2.6 For the purposes of precinct caucus lists and registration lists for municipal or special district elections, the residency requirement is based upon the date provided by the elector on his or her application.

2.26.1 The county clerk and recorder must enter the date provided by the elector in the registration record maintained in the statewide voter registration system. [Sections 1-3-101 and 31-10-201, C.R.S.]

2.26.2 If the elector submits an application and does not include the date he or she moved, the county clerk must enter the date the application is received or postmarked, whichever is earlier, as the date moved. But if the elector submits the application during the 22 days before an election and does not provide the date he or she moved, the county clerk must enter the date moved as the 22nd day before the election based upon the affidavit.

[Current Rule 2.8 is amended and moved to new Rule 2.2. Amendments are shown above. Portions of current Rule 2.14 are included in new Rule 2.2.4.]

2.3 Identification required from an applicant for voter registration

2.3.1 An applicant for voter registration must complete the identification number portion of the application for voter registration. But an applicant registering to vote in person is not required to show or present a Colorado driver’s license or ID if he or she provides a verifiable driver’s license or social security number.
(A) If the applicant cannot provide a verifiable driver’s license or social security number the applicant must show identification under section 1-1-104(19.5), C.R.S., when registering to vote, provide identification when voting in person, or provide a copy of identification when returning the mail ballot.

2.3.2 As used in section 1-1-104(19.5), C.R.S., government document means any document issued by a local, state or federal government, including:

(A) A paycheck from a government institution;

(B) A certificate of degree of Indian or Alaskan Native Blood;

(C) A letter from the director or administrator of a group residential facility that indicates that the elector is a resident of the facility and that he or she resides at the street address listed in the pollbook; or

(D) A division of youth corrections identification card issued by Department of Human Services.

[Sections 1-1-104(18.5), (19.5)(c), and (19.5)(d), C.R.S.]

2.3.3 As used in section 1-1-104(19.5)(a)(VII), C.R.S., current means that the date of the document is within 60 days of the date submitted for identification purposes unless the document states a longer billing cycle.

2.3.4 A suspended driver’s license is considered current and valid. A revoked or expired license is not considered current and valid and is not acceptable.

[Portions of current Rules 30.1.6(g), 30.1.7, 30.2.2, and 30.8 are included in new Rule 2.3.]

2.7.2.4 Treatment of applications where the required information was not provided

2.7.2.4.1 If an applicant fails to check the box(es) answering the question(s), “Are you a citizen of the United States?” or “Will you be 18 years of age on or before election day?”, the county clerk and recorder must accept and process the form shall be accepted for registration as complete so long as it is otherwise complete and the affirmation at the bottom of the form is signed.

2.7.2.4.2 If an applicant for voter registration fails to complete the required identification portion of the form in accordance with section 1-2-204(2)(f.5) and (3)(c), C.R.S., and rule 2.6.3, the county clerk must treat the application shall be treated as incomplete “incomplete”; however, but if the applicant submits a photocopy of his/her his or her driver’s license or identification card, then the county clerk may enter the ID number from the card into the
applicant’s record and consider—PROCESS the application AS COMPLETE “complete”.

2.7.3–2.4.3 If an applicant for voter registration fails to provide a date of birth the COUNTY CLERK MUST TREAT THE application shall be treated as INCOMPLETE “incomplete”; however, BUT if the applicant submits a photocopy of his/her HIS OR HER driver’s license or other approved form of ID which—that includes the date of birth, THEN the county CLERK MAY—MUST enter that information into the applicant’s record and consider—PROCESS the application AS COMPLETE “complete”.

(Current Rule 2.7 is amended and moved to new Rule 2.4. Amendments are shown above.)

2.10–2.5 Changes to an Elector’s Voter Registration Record

2.10.1–2.5.1 If an elector submits a change to his or her voter registration record that does not contain all of—and fails to include the information required by sections 1-2-216 or 1-2-219, C.R.S., the county clerk and recorder may—MUST not make the requested change, unless the county clerk and recorder can confidently identify the voter. OTHERWISE THE county clerk and recorder shall—MUST notify the voter what additional information is required to process the request.

2.10.2–2.5.2 If an elector submits a change to his or her voter registration record and writes or selects a name of an organization that is not a qualified political party or qualified political organization, or writes “none”, the elector’s affiliation shall—MUST be recorded as “Unaffiliated”.

2.10.3–2.5.3 If an elector submits a change to his or her voter registration record and leaves the affiliation section blank, THE COUNTY CLERK MUST MAKE no change will be made to the voter’s affiliation in the registration record.

2.5.4 WHEN THE COUNTY CLERK AND RECORDER PROVIDES A LIST OF ACTIVE ELECTORS TO A MUNICIPAL OR SPECIAL DISTRICT FOR AN ELECTION NOT COORDINATED WITH THE COUNTY, THE COUNTY CLERK AND RECORDER MUST REQUEST THE DESIGNATED ELECTION OFFICIAL OF THE MUNICIPALITY OR SPECIAL DISTRICT PROVIDE THE VOTE HISTORY INFORMATION FOLLOWING THE ELECTION. WITHIN TEN DAYS AFTER RECEIVING THE INFORMATION, THE COUNTY CLERK MUST ACTIVATE VOTER RECORDS AND REMOVE ID REQUIRED FLAGS IN SCORE AS PROVIDED IN SECTION 1-2-605(4)(B), C.R.S.

(Current Rule 2.10 is amended and moved to new Rule 2.5. Amendments are shown above.)

2.11–2.6 Changes to an elector’s voter registration status.

2.11.1–2.6.1 An elector may update his or her inactive registration status to active status by submitting:

(a) A signed written request, by mail, fax, or PDF attachment to an email;
(b) An online voter registration application; or

(c) An in-person request with identification.

[Section 1-2-605(4)(a), C.R.S.]

2.11.2–2.6.2 If an elector is unable to sign, another person must witness the elector’s mark. An elector may use a signature stamp because of age, disability, or other need. The stamp is treated as a signature and does not require a witness.

[Current Rule 2.11 is amended and moved to new Rule 2.6. Amendments between the current and new rule language are shown above.]

2.21–2.7 Minimum matching criteria

2.21.1–2.7.1 A record may not be transferred, consolidated, or cancelled unless the minimum matching criteria as set forth in sections 1-2-603 and 1-2-604, C.R.S., are met. If the minimum matching criteria are not met the county clerk may send a letter to the voter requesting confirmation of the missing or non-matching information in order to transfer, consolidate, or cancel the record.

2.21.2–2.7.2 For the purpose of sections 1-2-603 and 1-2-604, C.R.S., and this Rule a match of the name shall mean a match of the full name, except that the following shall be sufficient to establish a match:

(a) Common variations and nicknames in the first or middle name, i.e. Michael and Mike;

(b) Explainable and documented change of name, including last name, i.e. maiden name and married name; and

(c) Explainable and documented variations in suffix, except that the absence of a suffix in one of the records shall not be considered a variation. Examples of suffix variations that must be explained include junior in one record and III in another.

2.21.3–2.7.3 For the purpose of sections 1-2-603 and 1-2-604, C.R.S., and this Rule a match of the prior address shall mean a match of the residential street address.

2.21.4–2.7.4 The county clerk and recorder may use the DMV Motor Voter database to verify prior name or residence address history for the purpose of meeting the minimum matching criteria. The information gathered must be scanned and retained in the elector’s record in order to document how the criteria were met.
2.9-2.8  Registration of Homeless Voters
ELECTORS WHO HAVE NO FIXED PERMANENT HOME

2.9.1-2.8.1  For the purpose of voter registration residence a homeless voter may - AN ELECTOR WHO HAS NO FIXED PERMANENT HOME MUST identify a specific location within a precinct that the voter APPLICANT considers his OR HER home base.

(A) A HOME BASE IS A LOCATION THE APPLICANT to which the voter returns TO regularly and manifests an intent INTENDS to remain, and a place from which WHERE he or she can receive messages and be contacted.

(B) A home base may include a homeless shelter, a homeless provider, a park, a campground, a vacant lot, a business address, or any other physical location.

(C) FOR AN ELECTOR WHOSE HOME IS IN FORECLOSURE, THE ELECTOR MAY REGISTER TO VOTE OR REMAIN REGISTERED TO VOTE, AT THE FORECLOSED ADDRESS UNTIL THE ELECTOR ESTABLISHES A NEW PERMANENT RESIDENCE.

2.9.2-2.8.2  If the home base does not include a mailing address, THE APPLICANT then the homeless voter must provide a mailing address pursuant to IN ACCORDANCE with section 1-2-204(2)(f), C.R.S.

2.9.3-2.8.3  A post office box or general delivery at a post office shall not be deemed IS NOT a home base.

[Current Rule 2.9 is amended and moved to new Rule 2.8. Amendments are shown above.]
b. 2.10.2 Returns to the office of the county clerk and recorder a signed, notarized, and dated statement to the county clerk affirming that he or she believes the match was in error. The applicant must include his or her printed name, residential address, and date of birth on the signed, dated, and notarized statement.

[Current Rule 2.16 is amended and moved to new Rule 2.10. Amendments are shown above.]

2.17-2.11 20-DAY APPLICANTS UNDER SECTION 1-2-509(3), C.R.S.

2.11.1 When a county clerk and recorder deems an applicant “not registered” upon receipt of an undeliverable new voter notification in accordance with section 1-2-509(3), C.R.S., the applicant shall be mailed a confirmation card by forwardable mail. The confirmation card must meet the requirements of section 1-1-104(2.8), C.R.S. and shall have a postage prepaid returnable portion that is preaddressed to the sending county clerk and recorder.

2.17.1-2.11.2 If the county clerk and recorder receives an applicant returns the signed confirmation card within 90 days from an applicant who was deemed “not registered” in accordance with section 1-2-509(3), C.R.S., the applicant shall be deemed registered as of the date of the original application.

2.17.2 During the 28 days prior to an election, if an applicant who has been deemed “not registered” in accordance with section 1-2-509(3), C.R.S., completes a certificate of registration and presents identification in person at the office of the county clerk and recorder, the applicant shall be deemed registered as of the date of the original application.

2.11.3 During the 22 days before an election, the county clerk and recorder must defer processing undeliverable new voter notifications. After the election is closed, the clerk must deem an applicant “not registered” under section 1-2-509(3), C.R.S., only if the applicant did not vote in the election.

[Current Rule 2.17 is amended and moved to new Rule 2.11. Amendments are shown above.]

2.4-2.12 Confidentiality of Agency in Voter Registration

2.12.1 Information about the name and location of an agency for an application completed at a voter registration agency or driver’s license office is confidential. [42 USC §§ 1973gg-3(c)(2)(D)(iii)]

[Portions of current Rule 2.4 are included in new Rule 2.12.1.]

2.12.2 An elector may request his or her voter registration address be confidential under section 24-72-204(3.5), C.R.S., in person.
(A) The elector must use the application provided by the Secretary of State and include his or her name, address, and birth date on the application.

(B) The county clerk and recorder must not charge an additional processing fee if the elector changes his or her address.

[Portions of current Rule 2.5 are included in new Rule 2.12.2.]

2.12.3 Registration of Address Confidentiality Program (ACP) Electors

(A) When an ACP participant registers to vote by mail, the elector must provide a copy of his/her ACP Authorization Card.

(B) The county clerk and recorder must:

(i) Use the actual residence address of the ACP elector for precinct designation.

(ii) Use the substitute address, as defined in Section 24-30-2103(14), C.R.S., for all correspondence and mailings placed in the United States mail.

(iii) Keep the participant’s address, county, and voting precinct and split number confidential from the public.

(C) A state or local government agency may request access to an ACP participant’s voter registration record using the process in Section 24-30-2110, C.R.S.

(D) Except as specifically provided by Part 21 of Article 30 of Title 24, C.R.S., a program participant’s actual address and telephone number is not a public record under Part 2 of Article 72 of Title 24, C.R.S.

[Portions of current Rule 2.12 are included in new Rule 2.12.3.]

2.18.2.13 List Maintenance Pursuant to UNDER section 8 of the National Voter Registration Act of 1993

2.18.1.2.13.1 When the United States Postal Service returns a voter information card or confirmation card is returned to the county clerk as undeliverable, or provides the clerk with a postcard notice of mail forwarding is provided by the United States Postal Service to the county clerk and recorder, the county clerk and recorder shall mark the voter’s record “Inactive – returned mail” and shall mail a confirmation card. Where a confirmation card sent under this rule is returned as undeliverable, the county is not required to mail another card.
2.18.2  National Change of Address (NCOA). Counties may utilize the NCOA to send mailings to electors who may have moved to request that the electors update their voter registration records. However, no county may update the registration address of any registration record or change the status of an elector to “inactive” based solely upon the information provided by NCOA.

2.18.3  In accordance with section 1-2-605(7), C.R.S., no later than 90 days following a General Election, the county clerk and recorder in each county shall MUST cancel only the registrations of electors who have met the following requirements:

a. (A) Whose records have been marked “Inactive – returned mail”, “inactive INACTIVE – undeliverable”, or “Inactive – undeliverable ballot”, or INACTIVE – NCOA”;

b. (B) Who have been mailed a confirmation card; and

c. (C) Who have since failed to vote in two consecutive General elections.

2.13.5  An elector whose registration record was cancelled during the previous six years under section 1-2-605(7), C.R.S., and rule 2.12.2, may request reinstatement of the record. The elector must provide proof that he or she has continuously resided at the address shown on the registration record since the record was cancelled.

2.22  Effective January 1, 2012, no county may consolidate or cancel duplicate records in accordance with section 1-2-604, C.R.S., within the period beginning 90 days prior to a Primary or General Election.

[Current Rule 2.22 is amended and moved to new Rule 2.13. Amendments are shown above.]

2.14  Voter registration at a voter service and polling center

2.14.1  A person registering voters or updating voter registration information in a voter service and polling center must:

(A) Be a permanent or temporary employee of the county clerk and recorder’s office;

(B) Successfully pass the criminal background check described in rule 6.4. Any person who has been convicted of an election offense or an offense with an element of fraud is prohibited from handling voter registration applications or conducting voter registration and list maintenance activities; and

(C) Successfully complete a training course provided by the Secretary of State.
2.14.2 The person registering voters or updating voter registration information in a voter service and polling center must verbally confirm each elector’s name and residential address.

2.15 Voter registration records and data

2.15.1 Preservation of Voter Registration Records. Notwithstanding the retention timelines specified in section 1-2-227, C.R.S., the county clerk and recorder may destroy paper voter registration records as soon as they have been digitally recorded in the statewide voter registration database known as “SCORE”. Such records shall be retained. The statewide voter registration system must retain digital images of voter registration applications in perpetuity in digital format by the voter registration database in accordance with Title 1, C.R.S. and this rule.

2.15.2 After a receipt of request, the fee for providing the information shall be determined. The fee must be paid prior to the request being filled. Under section 24-21-104(3), C.R.S., the secretary of state must charge a fee for voter information reports and related services. A request for elections data must be submitted using the elections data request form. The secretary of state will provide the requested data after payment of the fee as outlined in the fee schedule on the secretary’s website.

2.15.3 The county clerk and recorder of each county may charge fees for county voter information reports and related services, such as the printing of labels provided by the centralized statewide registration system. However, but in accordance with federal requirements governing the use of federal funds, fees shall not exceed county direct and indirect costs for providing such reports and services.

2.15.4 Custodianship of Voter Registration Information

49.3.2-2.15.3 The county clerk and recorder of each county may charge fees for county voter information reports and related services, such as the printing of labels provided by the centralized statewide registration system. However, but in accordance with federal requirements governing the use of federal funds, fees shall not exceed county direct and indirect costs for providing such reports and services.

49.2-2.15.4 Custodianship of Voter Registration Information

49.2-2.15.4(a) The Secretary of State shall be the official custodian of the information contained in the centralized statewide registration system and the computerized statewide voter registration list created and maintained pursuant to section 1-2-301, C.R.S.

49.2-2.15.4(b) The county clerk and recorder for each county shall be the official custodian of the voter registration information only for electors within that county.
SCORE username and password administration

49.1.2.16.1 The state user administrator shall assign county administrator privileges to the individual designated in each county by the county clerk and recorder. The county clerk and recorder shall submit a request for county administrator privilege to the state user administrator in writing. The request specifically state the full name of the county employee that is being assigned as a county administrator.

49.1.2.16.2 Each county may have privileges assigned to no more than one (1) individual, except that any county clerk and recorder may apply to the Secretary of State for an additional county administrator.

49.1.2.16.3 The county administrator is responsible for security administration and shall assign all access privileges, as well as usernames and passwords for county employees and temporary election workers.

49.1.3.1.1 For county employees, the county administrator shall assign a unique username in accordance with the naming conventions provided by the Secretary of State.

49.1.3.2.1 Passwords shall be assigned by the county administrator upon initial authorization and shall be changed by users and maintained confidentially.

49.1.4.1.1 If a county employee or temporary election worker is no longer employed by the county, the county administrator shall inactivate the username within a reasonable timeframe, not to exceed one (1) business week.

Rule 3. Rules Concerning Qualified Political Organizations

3.2.1 The required proof of organization, which may be filed at any time after organization, shall include, but shall not be limited to, a QUALIFIED POLITICAL ORGANIZATION, AS
defined in Rule 1.1.1, must file proof of organization with the Secretary of State. The proof must include, but is not limited to:

a. 3.1.1 By laws of the Colorado political organization which shall define the organization’s bylaws, which must include the method for selecting officers, selecting delegates to county, state, and national conventions, and selecting candidates planning to petition onto the state’s general election ballot; and using the name of the Colorado political organization;

b. 3.1.2 The names, addresses, and telephone numbers of the elected organization’s Colorado chairperson, vice chairperson, and secretary, together with the names, addresses, and telephone numbers of all other members elected or appointed to other offices or committees authorized by the by-laws bylaws.

3.3.2 A qualified political organization shall must meet at least once a year.

3.3.3.1 During the meeting in the odd-numbered year, the organization must select shall be held for the purpose of selecting a chairperson, vice-chairperson, secretary, and other officers or committees as shall be provided for in the by-laws bylaws on file with the Secretary of State required by the organization’s bylaws.

(a) For new political organizations if the political organization is a new organization, the organization must hold this meeting must take place prior to before placing a candidate on the ballot. Therefore, this meeting may occur in this instance, the organization may hold this meeting in an even-numbered year and may select candidates as described in Rule 3.3.3.

3.3.3.2 The organization’s chairperson and the secretary shall must file with the Secretary of State a full and complete list, under oath, of the persons elected or appointed pursuant to Rule 3.2 under this Rule 3.2, together with any amendments to the by-laws bylaws adopted at the meeting.

3.3.3.3 During the meeting in the even-numbered year, the organization must select shall be held for the purpose of selecting candidates who wish to use the name of the political organization on petitions for the next general election.

(a) A political organization which has not yet been qualified may select its candidate at the same meeting where the officers of the organization are named.

3.4.3.3 To remain in good standing, a qualified political organization shall must place a candidate or candidates on the general election ballot every two years. A write-in candidate alone is not sufficient to meet this requirement.

3.4.1-3.3.1 Organization candidates wishing to represent a qualified political organization on the general election ballot shall be placed in nomination by
nominating petition pursuant to MUST BE NOMINATED IN ACCORDANCE WITH
section 1-4-802, C.R.S.

3.4-3.3.2 Each petition MUST contain the name of one candidate and shall have
attached an affidavit signed under oath by the chairperson and secretary of the
qualified political organization. The affidavit form MUST be approved by the
Secretary of State, and will include the date of the meetings required in Rule 3.3.

3.4-3.3.3 For a candidate To qualify for the ballot, the candidate must have been
affiliated with the qualified political organization for one year or, if the political
organization has not previously been qualified FOR ONE YEAR, the candidate must
have been registered as unaffiliated for one year.

3.4.4 Having the name of a candidate from the qualified political organization appear
on the ballot by the use of the write-in candidacy process shall not be considered
as, nor meeting the requirements of, placing a qualified candidate on the general
election ballot.

3.5-3.4 A political organization shall be qualified as soon as it THE SECRETARY OF STATE WILL
QUALIFY A POLITICAL ORGANIZATION IF THE ORGANIZATION:

(a)-3.4.1 Files proof of organization with the Secretary of State;
(b)-3.4.2 Meets to name AND NAMES a candidate to the general election ballot; and
(c)-3.4.3 Certifies a candidate to the general election ballot.

3.6-3.5 Once a political organization becomes a qualified political organization, eligible electors
shall be able to MAY register as affiliated AFFILIATE with the political organization.

3.6.1 When an individual appears at any office or location for the purpose of voter
registration, the questions asked and the information recorded shall be amended
to reflect “political organization” affiliation.

3.6.2 The opportunity to declare or change a political affiliation shall be provided
exactly as the law provides for political parties in sections 1-2-204(2)(j) and. 1-2-219, C.R.S.

3.6.3 At any time a declaration or change in affiliation is requested, the same
procedure shall be used for declaring a political party or political organization
affiliation.

3.6.4 In recording the information on the voter registration page, or affidavit, the
affiliation with a political organization shall be listed by the name entry of the
organization.

3.6.5 In converting information on the voter registration page to lists, submissions for
data entry, the Secretary of State’s master voter registration list, etc., standard
abbreviations shall be used and will be furnished to the county clerk and recorders by the Secretary of State.

3.7.3.6 The Secretary of State will revoke the qualified status of a political organization if the organization does not fully comply with Rules 3.3 and 3.4. shall lose their status as qualified political organizations by failing to do any one of the following:

(a) Meet in odd numbered years and file their list of officers with the Secretary of State, unless excused under Rule 3.3.1(a);

(b) Meet in even numbered years and select a candidate or candidates who wish to appear on the ballot at the next general election;

(c) Place a candidate on a general election ballot through a nominating petition, meeting the requirements of Rule 3.4.

3.8.3.7 If the Secretary of State revokes the qualified status of a political organization, the Secretary will notify the county clerk and recorders by June 1 of each odd-numbered year of the loss of qualified status of a political organization. Upon receiving notification, the county clerk and recorders shall mark on every affected voter registration record records as “unaffiliated”, where applicable.

3.9.3.8 Except for the precinct caucus list furnished to major political parties, a qualified political organization may obtain print-outs, lists, and tapes, etc. of voter registration records shall be furnished to qualified political organizations at the same rate or cost as charged to political parties. The only exception to this provision shall be the list furnished to the major political parties prior to the statutory precinct caucus day.

3.10.3.9 On all summary reports of voter registration by political party, the voter registration summary report shall list those registered with major political parties, minor political parties, qualified political organizations, or as unaffiliated categories.

3.11 Electors, whose voter registration record shows affiliation with a qualified political organization and who appear to vote at a primary election, shall complete a Declaration of Party Affiliation, thus losing affiliation with the qualified political organization.

Rule 4. Coordinated Elections

6.1.4.1 Participation in coordinated elections.

6.1.4.1.1 For elections where the electors do not need to be registered electors, political subdivisions may conduct their own elections and must coordinate with the coordinated election official any ballot issue notice required by Article X, Section 20 of the Colorado Constitution.

6.1.4.1.2 The affected coordinating political subdivision shall—must enter into
AN intergovernmental agreements AGREEMENT WITH THE COUNTY CLERK AND
RECORDER which—THAT delineate DELINEATES which tasks shall be—ARE the
responsibility of the designated election official of the political subdivision and
which shall be—ARE the responsibility of the coordinated election official
COUNTY CLERK AND RECORDER.

6.2.4.2 Procedures for Coordinated Elections Involving Jurisdictions Shared by Multiple
Counties

6.2.4.2.1 For each jurisdiction that is shared by multiple counties, a controlling
county MUST be designated for the purpose of assigning and coordinating
the ballot letter/number for the shared races, issues, and questions in
coordinated elections.

6.2.4.2.2 The controlling county IS the county where the administrative
office of the political subdivision is maintained at the time that the controlling
county is designated.

(a) If the administrative office is not maintained within the boundaries of the
political subdivision, the controlling county MUST be the county where
the largest number of active registered electors within the jurisdiction reside
at the time that the controlling county is designated.

(b) Once designated, the controlling county will not change unless approved by
the Secretary of State upon request of any of the affected counties.

6.2.3—Repealed.

6.2.4.2.3 The controlling county MUST coordinate with each county that shares
the jurisdiction to assign the ballot number/letter in accordance with Rule 6.5 no
later than the date of ballot certification. All counties within the shared
jurisdiction MUST ensure that the shared races, issues, and questions are
printed on the ballot as certified by the Secretary of State or designated election
official, and in the order assigned by the controlling county

6.2.5.4.2.4 If any controlling county fails to fulfill its responsibilities in accordance
with this Rule, any of the other counties in the shared jurisdiction may make a
written request to the Secretary of State to temporarily assume the duties of the
controlling county. The Secretary of State MAY act on
behalf of the controlling county or to temporarily designate another county to
act as the controlling county in order to IMPLEMENT assure implementation of
this Rule.

6.3.4.3 Form of election for November coordinated elections.

6.3.1.4.3.1 The county clerk and recorder is the election official for coordinated
elections which are—held in November of each year AND IS RESPONSIBLE FOR
MAILING THE ARTICLE X, SECTION 20 BALLOT ISSUE NOTICE.
(a) The county clerk and recorder shall be responsible for mailing the Article X, Section 20 Ballot Issue notice.

(b) The county clerk and recorder shall not be required to conduct more than one form of election unless he or she so chooses.

6.3.2 School districts that have the opportunity to participate in a coordinated election may not elect to hold separate mail ballot elections but must participate in the form of election chosen by the county clerk and recorder.

21.1-4.3.2 Placing measures on the ballot for coordinated odd-year elections.

21.1.1 (A) For a statewide election, the Secretary of State MUST determine whether the proposed initiative is eligible to appear on an odd-year election ballot and WHETHER IT concerns state matters arising under Section 20 of Article X of the State Constitution.

21.1.2 (B) For election concerning county or other political subdivision ALL OTHER ELECTIONS, if the election is held as a coordinated election each THE political subdivision CONDUCTING THE ELECTION MUST determine whether the proposed initiative or referred measure is a local government matter arising under Section 20 of Article X of the State Constitution.

[Current Rule 21.1 is amended and moved to new Rule 4.3.2. Amendments between the current and new rule language are shown above.]

6.4.4 Form of coordinated elections held other than in November.

6.4.4.1 For all other elections where political subdivisions hold an election on the same day, the electors or boundaries overlap and ballot issues as defined in Section 1-1-104 (2.3), C.R.S., appear on the ballot of overlapping jurisdictions, the governing bodies or the designated election officials of such THE overlapping jurisdictions must name a coordinated election official who is responsible for assuring that the Article X, Section 20 notice is given.

6.4.2-4.4.2 The political subdivisions may contract with the appropriate county clerk and recorder to be the coordinated election official.

6.5.4.5 Determination of ballot issues and texts.

6.5.4.1 Each political subdivision MUST prepare the list of candidates and the ballot title and text for ballot issues and ballot questions, as required by law.

(a) The coordinated election official MUST assure that PRINT the ballot title is on each ballot as required by law.

(b) Political subdivisions may only require the coordinated election official to
print the entire text of a ballot issue or ballot question on the ballot if they pay.

THE POLITICAL SUBDIVISION pays for any additional cost associated with printing and if sufficient space is on the voting equipment to print the entire text given the other issues, questions, and candidates on the ballot. The coordinated election official shall MUST tell the political subdivision how much space is available for text for each position on the ballot. If the required ballot title and text is too long for the voting equipment, the coordinated election official may choose to conduct the election with a different form of ballot.

(c) For counties where ballot election material must be printed in languages other than English, the political subdivisions are responsible for assuring proper translation of all election materials related to that political subdivision and must pay their pro-rata share of increased printing costs unless otherwise provided by the intergovernmental agreement.

(d) For counties where election material is not required to be printed in languages other than English, the political subdivisions are not required to provide translation of all election materials nor pay a pro-rata share of the printing costs unless they so agree.

6.5.2.4.5.2 Each political subdivision shall MUST determine the order of the ballot issues for their political subdivision in accordance with the requirements of Colorado Constitution Article X, Section 20 and Title 1.

(a) Referred measures shall MUST be designated by a letter or by a number and a letter; initiatives shall be designated by a number.

(b) For each grouping of ballot issues and ballot questions by a political subdivision, all referred measures shall MUST precede all initiatives.

(c) For each grouping of ballot issues and ballot questions, the order shall be as follows:

1. (I) Referred measures to increase taxes;
2. (II) Referred measures to retain excess revenues;
3. (III) Referred measures to increase debt;
4. (IV) Other referred measures;
5. (V) Initiatives to increase taxes;
6. (VI) Initiatives to retain excess revenues;
7. (VII) Initiatives to increase debt;
§-(VIII) Other citizen petitions.

(d) For statewide measures, initiatives shall—MUST be numbered in the order in which the statements of sufficiency are issued. The numbers one through five shall—MUST be reserved for initiatives to increase taxes; the numbers six through ten shall—MUST be reserved for initiatives to retain excess revenues; the numbers eleven through fifteen shall—MUST be reserved for initiatives to increase debt; all other citizen petitions shall—MUST be numbered consecutively beginning with sixteen.

(e) In accordance with section 1-5-407(5)(b), C.R.S., whether initiated or referred, every proposed change to the Colorado Constitution shall—MUST be called an “amendment” and every proposed change to the Colorado Revised Statutes shall—MUST be called a “proposition”

(f) Ballot issues from the various political subdivisions shall—MUST be ordered on the ballot as provided in section 1-5-407(5), C.R.S:

1. (I) Each category of referred and initiated state amendments and propositions shall—MUST be numbered and listed on the ballot in the following series:

<table>
<thead>
<tr>
<th>A-Z</th>
<th>State Referred Constitutional Amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-99</td>
<td>State Initiated Constitutional Amendments</td>
</tr>
<tr>
<td>AA-ZZ</td>
<td>State Referred Statutory Propositions</td>
</tr>
<tr>
<td>101-199</td>
<td>State Initiated Statutory Propositions</td>
</tr>
</tbody>
</table>

If a referred or initiated measure contains both a proposed constitutional and statutory change, the measure shall—MUST be ordered on the ballot as a constitutional amendment.

2. (II) Each category of initiated local ballot issues and questions shall—MUST be numbered in the following series:

<table>
<thead>
<tr>
<th>200-299</th>
<th>County Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>300-399</td>
<td>Municipal Issues</td>
</tr>
<tr>
<td>400-499</td>
<td>School District Issues</td>
</tr>
<tr>
<td>500-599</td>
<td>Ballot Issues and Questions for other political subdivisions greater than a county.</td>
</tr>
<tr>
<td>600-699</td>
<td>Ballot Issues and Questions for other political subdivisions which are wholly within a county.</td>
</tr>
</tbody>
</table>
3.–(III) Each category of local referred ballot issues and questions shall
MUST be designated by a letter or a number and a letter in the
following series:

<table>
<thead>
<tr>
<th>1A-1Z</th>
<th>County Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>2A-2Z</td>
<td>Municipal Issues</td>
</tr>
<tr>
<td>3A-3Z</td>
<td>School District Issues</td>
</tr>
<tr>
<td>4A-4Z</td>
<td>Ballot Issues and Questions for other political subdivisions greater than a county.</td>
</tr>
<tr>
<td>5A-5Z</td>
<td>Ballot Issues and Questions for other political subdivisions which are wholly within a county.</td>
</tr>
</tbody>
</table>

4.–(IV) Ballot questions and issues are numbered or lettered in the order in
which the measures are certified to the ballot by the designated election
official after the protest period has ended, or if a protest was filed after
the protest has been completed.

5.–(V) For other than state issues, if a county has multiple cities and/or
multiple discrete school districts and other political subdivisions, the
designated election official may either further subdivide the series and
assign each political subdivision a specific series of numbers, or when
the ballot is certified the designated election official may assign the final
numbers/–OR letters, making sure that all measures for each political
subdivision are grouped together.

6.–(VI) For other than state issues and questions, if the same ballot issue or
question will be on the ballot in more than one county, the county clerks
shall MUST confer with one another and shall MUST give the same ballot
number or letter to the ballot issue or questions.

7.–(VII) Each ballot question or issue shall MUST contain the name of the
political subdivision at the beginning of the ballot questions or issue. If
the designated election official chooses, the name of the political
subdivision may appear before the grouping of questions, such as State
Ballot Questions, Arapahoe County Ballot Questions, City of Aurora
Ballot Questions, etc.

4.6 CANDIDATE AUDIO RECORDINGS

4.6.1 Candidates whose names are listed on a ballot A CANDIDATE FOR
STATEWIDE OFFICE, THE GENERAL ASSEMBLY, CONGRESSIONAL OFFICE, REGENT,
OR DISTRICT ATTORNEY must provide an audio recording of the pronunciation of
their HIS OR HER name to the Secretary of State, prior to the election for offices
that are voted on by the electors of the entire state, or of a congressional district,
or for the offices of members of the general assembly or district attorney or a
district office of state concern. The candidate must record his or her name exactly as it appears on the candidate acceptance form, statement of intent, or declaration of intent to run for retention in a judicial office, as applicable, and the candidate must provide the recording to the secretary of state no later than the deadline to file the candidate acceptance form, statement of intent, or declaration of intent to run for retention in a judicial office, as applicable.

[Rules 10.4.1 through 10.4.4 are repealed and consolidated into Rule 4.6.1]

10.5.4.6.2 A candidate for a county, municipal, school district, and or special district candidates whose names are listed on a ballot for in an election coordinated by the county clerk and recorder must provide an audio recording of the pronunciation of their his or her name to the county clerk and recorder prior to the election for offices that are voted on by the electors of the county, municipality, school district, or special district. The candidate must record his or her name exactly as it appears on the statement of intent, and must provide the recording to the county clerk and recorder no later than the deadline to file the statement of intent.

[Rules 10.5.1 through 10.5.2 are repealed and consolidated into Rule 4.6.2]

4.7 Congressional term limits declaration

24.1 4.7.1 The Secretary of State shall make the Congressional Term Limits Declaration available to every candidate for United States House of Representatives or the United States Senate, the Congressional Term Limits Declaration—provided in Article XVIII, Section 12a of the Colorado Constitution. The Secretary of State will offer the Congressional Term Limits Declaration to every such candidate when the candidate files his or her candidate affidavit with the Secretary of State. Any failure of the Secretary of State to offer the Congressional Term Limits Declaration to a candidate shall have no effect on such the candidate’s candidacy.

24.2 4.7.2 The Secretary of State must accept Part A of the Term Limits Declaration shall be accepted by the Secretary of State if Part B of the Term Limits Declaration has not been was not duly executed and submitted. Art. XVIII, sec. 12a (7)

24.3 4.7.3 In the case of a candidate who has qualified as a candidate for a term that would exceed the number of terms set forth in Term Limits Declaration One, the Secretary of State shall not place the words, "Signed declaration to limit service to [3 terms] [2 terms]" after the candidate’s name, even if the candidate has executed and submitted Parts A and B of Term Limits Declaration One.

[Current Rule 24 is amended and moved to new Rule 4.7. Amendments are shown above.]
4.8 BALLOT FORMAT AND PRINTING

4.8.1 The text of all ballot issues that are subject to Article X, Section 20 shall be printed in all capital letters. The names of all candidates and all other ballot issues and questions shall be printed in upper and lower case. The county clerk and recorder must print the candidate names and the text of ballot issues and ballot questions in upper and lower case, except that the clerk and recorder must print the text of ballot issues subject to Article X, Section 20 of the Colorado Constitution in all uppercase text.

4.8.2 If there is no candidate on the ballot for any particular office, the ballot shall read “No candidate for this office.”

[Current Rules 10.1 and 10.3 are amended and moved to new Rules 4.8.1 and 4.8.2. Amendments are shown above.]

4.8.3 Printing primary election ballots.

4.8.3.1 If a major political party, as defined in section 1-1-104(22.5), C.R.S., nominates more than one candidate for any office, the county clerk and recorder must conduct the primary election for all major political parties.

(a)(I) The county clerk must include on the ballot all offices to which candidates may be nominated in the primary election.

(b)(II) If there are no candidates for any particular office, the county clerk must print on the ballot “There are no candidates for this office”.

[Sections 1-4-101 and 1-4-104.5, C.R.S.; Election Rule 10.3]

4.8.3.2 If a minor political party, as defined in section 1-1-104(23), C.R.S., has nominates more than one candidate for any office, the county clerk and recorder may conduct the primary election for that party only.

(a)(I) The county clerk must include on the ballot only the offices for which there is more than one candidate designated.

(b)(II) If there is only one minor party candidate designated for any office, the candidate will be certified to the general election ballot.

[Sections 1-4-101, 1-4-104.5(3), and 1-4-1304, C.R.S.]

[Current Rule 10.6 is amended and moved to new Rule 4.8.3. Amendments are shown above.]

4.8.4 Use of unique numbers on ballots.
10.8.1 (A) Except for ballots sent to military or overseas electors by electronic transmission under Rule 16.2, no county may NOT print a ballot for use in a state or federal election that has a unique number, or a barcode containing a unique number, that is specific to a single ballot.

(a) (i) A county that uses rotating numbers must print at least ten ballots of each ballot style for each number.

(b) (ii) Nothing in this rule prohibits a county from printing a unique number or barcode on the removable stub.

10.8.2 (B) After an election judges have dissociated a voted ballot from its envelope and removes the stub, it is removed, the county may write or print unique numbers on the voted ballot for auditing and accounting purposes, including duplication of damaged ballots and risk limiting audits.

10.8.3 (C) For ballots printed before the adoption of this rule that are in a county’s possession, the county must redact unique numbers, or barcodes containing unique numbers, before providing ballots in response to a request for inspection under the Colorado Open Records Act (Section 24-72-205.5(4)(b)(II), C.R.S.).

[Current Rule 10.8 is amended and moved to new Rule 4.8.4. Amendments are shown above.]

4.8.5 If a ballot has been printed in error, the designated election official shall consult, as soon as the error is discovered, with the Secretary of State and follow the direction of the Secretary of State on the appropriate method of correction. IF THE DESIGNATED ELECTION OFFICIAL DISCOVERS A BALLOT ERROR, HE OR SHE MUST IMMEDIATELY SEEK AND FOLLOW THE SECRETARY OF STATE’S ADVICE ON HOW TO CORRECT THE ERROR.

[Current Rule 10.2 is amended and moved to new Rule 4.8.5. Amendments are shown above.]

6.6.9 Colorado Constitution Article X, Section 20 notice requirements.

6.6.1-4.9.1 The state and local governments, excluding enterprises, have sole responsibility for drafting and distribution of the notice required by Article X, Section 20. Any or all of the THESE responsibilities may be delegated to the coordinated election official in the intergovernmental agreement.

6.6.2-4.9.2 The notice shall MUST be mailed to “All Registered Voters” at the mailing addresses of active registered electors in the county, as indicated on the voting record IN SCORE.

(a) Nothing shall preclude the coordinated or designated election
official from sending notice of various elections to persons who are not eligible electors if the notice sent is part of the coordinated notice and if the sending arises from the official’s efforts to mail the notice at “least cost”.

(b) Nothing shall preclude the coordinated or designated election official from sending notice to each household in the county or political subdivision whether or not registered electors reside at that household as long as notice is sent which ensures that all active registered electors are included on the mailing list.

(c) Nothing shall preclude the coordinated or designated election official from sending notice to each registered elector in a particular political subdivision.

(a)-(d) The coordinated or designated election official may include the following statement with the ballot issue notice: “This notice is mailed to each address with one or more active, registered electors. You may not be eligible to vote on all issues presented in this notice.”

[Current Rule 6.5.3(a) is amended and moved to new Rule 4.9.2(d). Amendments are shown above.]

6.6.3-4.9.3 The coordinated election official must include information in the package sent with the notice that tells electors whether the election is a mail ballot election, a polling place election, a vote center election or a combination of election forms.

(a) If the election is a polling place election or a vote center election, the notice of the location of the polling place or vote center may be included in the consolidated mailing.

(b) If a separate mail ballot election is being held by a political subdivision in the county at the same time as a polling place election or a vote center election, the notice shall include that information. Section 1-5-205, C.R.S.

(b) The coordinated or designated election official may include the following statement on the ballot issue notice: “The following is a summary of comments filed in favor of, or opposed to, the ballot issue.”

[Current Rule 6.5.3(b) is amended and moved to new Rule 4.9.3(b). Amendments are shown above.]

6.6.4-4.9.4 If state statute allows the ballot issue notice and the ballot to be mailed at the same time, the ballot for the mail ballot election may be included with the notice.

6.6.5-4.9.5 The political subdivisions must provide all completed Article X, Section
20 notices in camera ready format or as otherwise specified.

6.6.6.4.9.6 The coordinated election official shall not be responsible for failure to meet the Article X, Section 20 constraints if the POLITICAL SUBDIVISION FAILS TO SUBMIT THE notice and summaries are not submitted by the political subdivision within the deadline and in the form required by the coordinated election official.

(a) The summaries of comments for and against ballot issues shall—MUST not include language of a generally recognized profane, indecent, immoral, offensive, scandalous or libelous character. No names of persons or private groups shall be included in any summary.

(b) For purposes of counting words and to verify the five hundred constitutional limit for each “pro” and each “con” summary, a hyphenated word, unless it is divided by a continuation hyphen at the end of a line, counts as two or more words. A number counts as one word, regardless of dollar signs, commas or periods within the number.

6.7.4.9.7 Written—NO PERSON MAY WITHDRAW WRITTEN comments concerning ballot issues submitted to the designated election official for the political subdivision shall not be withdrawn after the end of the business day on the last Friday immediately preceding the forty-fifth day before the election.

[Current Rules 6, 10, and 21 are amended and moved to new Rule 4. Amendments are shown above.]

Rule 5. Rules Concerning Non-Partisan NONPARTISAN Elections not Coordinated by the County Clerk

5.2 MAIL BALLOT ELECTIONS

5.2.1 IF A POLITICAL SUBDIVISION COORDINATES WITH THE COUNTY CLERK AND RECORDER, THE DESIGNATED ELECTION OFFICIAL IS NOT REQUIRED TO SUBMIT A
SEPARATE MAIL BALLOT PLAN FOR THE ELECTION.

[Portions of current Rule 12.1.2 are included in new Rule 5.2.1.]

12.4.1.5.2.2 Coordinated and non-partisan elections. (a) Written plan. The IF A LOCAL GOVERNING BOARD DETERMINES AN ELECTION WILL BE CONDUCTED BY MAIL BALLOT, THE designated election official must submit a mail ballot plan to the Secretary of State no later than 55 days before any nonpartisan THE election, and 90 days before any election that is coordinated with or conducted by the county clerk and recorder. The designated election official must use the approved mail ballot plan template. that includes the following:

(A) THE DESIGNATED ELECTION OFFICIAL MUST INCLUDE AN ACTUAL SAMPLE OF THE SECRECY SLEEVE OR SECRECY ENVELOPE THAT THE DESIGNATED ELECTION OFFICIAL PLANS TO USE IN THE ELECTION.

(B) A HOME RULE MUNICIPALITY MUST CHECK THE APPROPRIATE BOX ON THE PLAN INDICATING WHETHER THERE ARE LOCALLY ADOPTED ELECTION PROCEDURES DIFFERENT FROM THOSE SET FORTH IN TITLE 1, C.R.S. THE SECRETARY OF STATE WILL NOT REVIEW THE MAIL BALLOT PLAN OF ANY HOME RULE MUNICIPALITY THAT FAILS TO INCLUDE THIS INFORMATION.

[Current Rule 12.4.1(a) is amended and moved to new Rule 5.2.2. Amendments between the current and new rule language are shown above.]

5.2.3 BALLOTS AND BALLOT PACKETS

(A) IN ANY ELECTION WHERE A MULTIPLE PAGE PRINTED BALLOT IS USED, A VOTER MUST VOTE AND RETURN ALL PAGES OF THE BALLOT AT THE SAME TIME. ANY VOTER WHO HAS RETURNED AT LEAST ONE PAGE OF A MULTIPLE PAGE PRINTED BALLOT WILL BE CONSIDERED TO HAVE VOTED.

12.5.2 (B) For non-partisan elections where multiple ballots will be included in the same packet or will be sent in separate packets, the ballots and return envelopes shall—MUST include distinctive markings or colors to identify political subdivisions when the colors or distinctive markings will aid in the distribution and tabulation of the ballots.

12.5.3 (C) The designated election official for each political subdivision for whom one or more county clerk and recorders are conducting the election shall assure that MUST PROVIDE a complete list of eligible electors in their political subdivision is sent to each appropriate county clerk and recorder, unless otherwise provided in the intergovernmental agreement. The political subdivision shall—MUST list each elector only once to assure ENSURE that each elector receives one and only one ballot unless otherwise authorized.
[Current Rules 12.5.2 and 12.5.3 are amended and moved to new Rule 5.2.3. Amendments between the current and new rule language are shown above.]

12.7.4 (D) All election materials prepared by the designated election official, including the Article X, Section 20 notice, may be included in the mail-in ballot packet.

[Current Rule 13.1 is moved to new Rule 5.2.3.]

13.1 (D) All election materials prepared by the designated election official, including the Article X, Section 20 notice, may be included in the mail-in ballot packet.

[Current Rule 13.1 is moved to new Rule 5.2.3.]

5.2.4 RECALL ELECTIONS. THE DESIGNATED ELECTION OFFICIAL MUST SUBMIT A WRITTEN PLAN TO THE SECRETARY OF STATE WITHIN FIVE DAYS AFTER THE DESIGNATED ELECTION OFFICIAL SETS THE DATE OF THE ELECTION. THE SECRETARY OF STATE WILL APPROVE OR DISAPPROVE THE PLAN WITHIN FIVE DAYS FROM THE DATE IT IS RECEIVED. [SECTION 1-12-111.5, C.R.S.]

[Portions of current Rule 12.4(b) are included in new Rule 5.2.4]
5.2.5.4 If there are no appropriate polling place locations, the designated election official for the political subdivision is unable to establish a voter service and polling center within the political subdivision, conducting the election, a polling place may be designated. The designated election official may designate a voter service and polling center outside of the political subdivision if the location that is convenient for the eligible electors of such political subdivision.

5.3.5.5 For elections not conducted in November and not coordinated with the county clerk and recorder, the ballot issue or question shall be identified by the name of the jurisdiction submitting the ballot issue or ballot question followed by a number in the case of initiatives or by a letter in the case of referred measures. For ballot issues and ballot questions in an election not coordinated with the county clerk and recorder, the designated election official must use the title and lettering style for statewide ballot issues and ballot questions specified in section 1-5-407 (5.3) and (5.4), C.R.S.

5.4.5.6 Elections authorized under Part 1, Article 45 of Title 37, C.R.S., (Water Conservancy Act), shall must be conducted in accordance with Articles 1 through 13 of Title 1, C.R.S., where applicable, unless otherwise ordered by the district court having jurisdiction over the water conservancy district, pursuant to section 37-45-103 (3), C.R.S. (“Court”).

5.4.1.5.1 The form and verification of any petition requesting an election conducted by a water conservancy district pursuant to sections 37-45-114 (2) and 37-45-136(3.5), C.R.S., (“Petition”), shall must conform with the requirements of sections 1-40-113 and 1-40-116, C.R.S., and the sections cited therein, and Rule 17 15 of these rules; except that petitioners need not seek petition format approval from the Secretary of State. The petition must be filed with the Court and the verification process shall be directed by the water conservancy district named in the petition, unless otherwise ordered by the Court.

5.4.2.5.2 The procedures for issuing the statement of sufficiency or insufficiency of the petition shall must conform to the requirements of section 1-40-117, C.R.S., and Rule 18 15 of these rules; except that the statement shall must be issued by the water conservancy district named in the petition, unless otherwise ordered by the Court.

5.4.3.5.4 The procedures for cure of a petition deemed insufficient shall must conform to the requirements of section 1-40-117, C.R.S., and Rule 19 15 of these rules; except any addendum to the petition shall must be filed with both the Court and the water conservancy district named in the petition, unless otherwise ordered by the Court.
5.4.4-5.6.5 The procedures for protesting the determination that a petition is insufficient shall MUST conform to the requirements of section 1-40-118, C.R.S., and Rule 20-15 hereof, unless otherwise ordered by the Court.

5.4.5-5.6.5 The designated election official MUST CONDUCT any election pursuant to section 37-45-114(2), C.R.S., shall be conducted no more than one hundred (100) days nor less than sixty (60) after the sixty-sixth but before the one hundredth day after from the date of the Court order, regardless of the actual expiration date of the term of the office, unless the Court order establishes an alternate date or the water conservancy district has notified the Court that such election is to be conducted as a coordinated election pursuant to section 1-7-116, C.R.S.

5.4.6-5.6.6 The form and procedures for filing candidate nomination forms and call for candidate nominations of persons desiring to be a candidate for the office to be voted upon at the Court-ordered election described in Rule 5.4.5, shall be in conformance with the form and procedures required for special districts MUST BE CONDUCTED under Article 1, Title 32, C.R.S., unless otherwise ordered by the Court.

5.5-5.6 Non-Partisan Elections: Polling Place Procedures.

5.5.1-5.6.1 For polling place elections being conducted in accordance with Article 1, Title 32, C.R.S., upon execution of the self-affirming oath or affirmation pursuant to section 32-1-806(2), C.R.S., the eligible elector desiring to vote shall MUST show his or her identification as defined in section 1-1-104(19.5), C.R.S., to one of the election judges. See section 1-7-110(1), C.R.S.

5.5.2 If the eligible elector has executed the self-affirming oath or affirmation and provided his or her identification, such eligible elector may be allowed to vote, if such vote is not challenged. See sections 1-7-110(2) and 32-1-806(4), C.R.S.

5.5.3-5.6.2 The election supplies provided to the supply judge of each polling place shall include an adequate number of provisional ballot envelopes that include the affidavit set forth in Rule 26.8. The designated election official MUST ENSURE THAT EACH POLLING PLACE HAS AN ADEQUATE NUMBER OF PROVISIONAL BALLOTS.

5.5.4 The signature and date on the provisional ballot affidavit envelope shall remain on the outside of the envelope.

5.5.6 The provisional ballot affidavit envelope shall be numbered to correspond to the number of the provisional elector's name in the poll book, and the word "provisional" shall be marked on the ballot.

5.5.7-5.6.3 Verification of Information in Provisional Ballot Affidavit. The designated election official shall verify the information contained in the provisional ballot.
affidavit pursuant to Rule 26. If the information contained in the affidavit provides adequate criteria such that the designated election official, using the Rule 26 search, can ascertain the registration of the elector, the provisional ballot shall count. If the information cannot be verified, the ballot shall be rejected. See MUST FOLLOW THE PROVISIONAL BALLOT PROCEDURES CONTAINED IN ARTICLES 1 THROUGH 13 OF TITLE 1 sections 1-8.5-105 and 1-8.5-106, C.R.S., and Rule 26.

5.5.8 The verification and counting of all provisional ballots shall be completed prior to the certification of the official abstract of votes cast in the election by the canvass board, pursuant to Section 1-10-203(1), C.R.S.

5.5.9 Canvassing Board’s Count of Provisional Ballots. If, after the expiration of twelve days following an election, the election judges cannot complete the count of the provisional ballots cast, the canvassing board appointed pursuant to Section 1-10-201(1.5), C.R.S., shall complete the count of such provisional ballots.

5.5.10 If 25 or more provisional ballots have been cast and counted, the results shall be reported as one total. If less than 25 provisional ballots have been cast and counted, the results shall be included in the results of the mail-in ballots counted in the election.

5.5.11 The provisional ballot shall not be counted if the elector failed to complete the affidavit on the envelope or the elector was not registered by the deadline in the State of Colorado.

5.5.12 A copy of the provisional ballot affidavit shall be provided to the county clerk and recorder of the county of the elector’s residence, and shall constitute a voter registration for future elections. See section 1-8.5-108, C.R.S.

5.7 THE COUNTY CLERK AND RECORDER FOR A COUNTY THAT CONTAINS ANY PORTION OF A POLITICAL SUBDIVISION WITHIN ITS BORDERS MUST PROVIDE ELECTION DAY REGISTRATION FOR THE POLITICAL SUBDIVISION.

5.7.1 THE COUNTY CLERK AND RECORDER MUST PROVIDE VOTER REGISTRATION THROUGH THE 22-DAY ELECTION PERIOD DURING NORMAL BUSINESS HOURS, MONDAY THROUGH FRIDAY, AND 7:00 AM TO 7:00 PM ON ELECTION DAY.

5.7.2 THE COUNTY CLERK AND RECORDER MUST PROVIDE DAILY REGISTRATION UPDATES 22 DAYS THROUGH THE DAY BEFORE ELECTION DAY, TO THE DESIGNATED ELECTION OFFICIAL BY SECURE TRANSMISSION AS OUTLINED IN RULE 43 AND PROVIDE A CERTIFICATE OF REGISTRATION TO THE APPLICANT ON ELECTION DAY

5.7.3 ON ELECTION DAY, THE COUNTY CLERK AND RECORDER MUST PROVIDE A CERTIFICATE OF REGISTRATION TO ANY ELECTOR WHO registers TO VOTE OR UPDATES HIS OR HER REGISTRATION.
Rule 6. Rules Concerning Election Judges

28.1-6.1 For purposes of training election judges, an “election cycle” shall mean all elections held during a calendar year beginning with January 1 and ending December 31.

28.2-6.2 In lieu of the oath for other election judges prescribed in section 1-6-114, C.R.S., each person appointed to serve as a student election judge shall take a self-affirming oath or affirmation before beginning their duties serving as a student election judge, in substantially the following form:

“I, __________________ do solemnly swear (or affirm) that I am a citizen of the United States and state of Colorado; that I am at least 16 years of age and a High School Junior or Senior; that I will perform the duties of an election judge according to law and to the best of my ability; that I will studiously strive to prevent fraud, deceit, and abuse in conducting the same; that I will not try to determine how any elector voted, nor will I disclose how any elector voted if in the discharge of my duties as a student election judge such knowledge shall come to me, unless called upon to disclose the same before some court of justice; that I have never been convicted of election fraud, any other election offense, or fraud and that, if any ballots are counted before the polls close on the date of the election, I will not disclose the result of the votes until after the polls have closed and the results are formally announced by the designated election official.”

6.3 A supervisor judge in a voter service and polling center must:

a. Successfully pass the criminal background check described in Rule 28.5. Any person who has been convicted of an election offense or fraud is prohibited from handle voter registration applications or conduct voter registration and list maintenance activities.

b. Successfully complete a training course provided by the Secretary of State.

6.4 The county clerk and recorder must arrange for a criminal background check on a supervisor judge and any a person registering voters in a voter service and polling center. The criminal background check must be conducted by the Colorado Bureau of Investigation in the Department of Public Safety or by the County Sheriff’s Department for the county in which the county clerk and recorder’s office is located.

[Current Rule 28 is amended and moved to new Rule 6. Amendments are shown above.]

Rule 7. Elections Conducted by the County Clerk and Recorder

7.1 Mail ballot plans

(a) 7.1.1 Written plan. The for every election conducted by the county clerk and recorder, the clerk must submit a mail ballot plan to the Secretary of State by
EMAIL no later than 90 days before the election. The county clerk must use the approved mail ballot plan template, that includes the following:

(A) FOR RECALL ELECTIONS, THE COUNTY CLERK MUST SUBMIT A MAIL BALLOT PLAN TO THE SECRETARY OF STATE BY EMAIL WITHIN FIVE DAYS AFTER THE APPROPRIATE OFFICIAL SETS THE ELECTION. WITHIN FIVE DAYS AFTER RECEIVING THE RECALL ELECTION PLAN, THE SECRETARY OF STATE WILL APPROVE OR DISAPPROVE.

(B) THE COUNTY CLERK MUST SUBMIT WITH THE MAIL BALLOT PLAN THE SECRECY SLEEVE OR ENVELOPE THAT THE CLERK INTENDS TO USE IN THE ELECTION.

[Current Rule 12.4.2(a) is amended and moved to new Rule 7.1. Amendments are shown above.]

42.4.3-7.1.2 Approval of mail ballot plans and submission of amendments

(a) If the Secretary of State requests modifications to a plan prior to approval, the designated election official shall submit the modified plan within ten days from the request. The secretary of state will approve or disapprove the modified plan within 15 days from the date it is received.

(b) A designated election official shall submit a security plan outlining the amendment(s) to the plan. The amendment must state the specific section of the plan amended and the reason(s) for the amendment. The secretary of state will approve or disapprove the amendment within 15 days from the date it is received. If the amendment is received within 30 days before the election, the Secretary of State will approve or disapprove the amendment within two business days.

[Current Rule 12.4.3 is amended and moved to new Rule 7.1.2. Amendments are shown above.]

42.3.3-7.1.3 For elections coordinated by THE county clerk and recorder, MUST SUBMIT a security plan in accordance with Rule 43 in addition to the mail ballot plan submitted in accordance with this Rule.

[Current Rule 12.3.3 is amended and moved to new Rule 7.1.3. Amendments are shown above.]

42.5-7.2 Ballots

42.5-7.2.1 In any election where a multiple page printed ballot is used, a voter must vote and return all pages of the ballot at the same time. Any voter who has returned at least one page of a multiple page printed ballot will be considered to
have voted.

[Current Rule 12.5.1 is amended and moved to new Rule 7.2.1]

12.5.5.7.2.2 In accordance with section 1-7-116(1), C.R.S., for all Coordinated elections, the outgoing envelope as well as the instructions or other notice shall MUST include a notice advising electors that they may receive a ballot from another political subdivision conducting a mail ballot election.

12.5.6.7.2.3 If the ballot is returned to the election official as undeliverable, the official shall not be COUNTY CLERK AND RECORDER IS NOT required to re-mail the ballot packet.

[Current Rules 12.5.5 and 12.5.6 are amended and moved to new Rules 7.2.2 and 7.2.3]

7.2.4 IN ACCORDANCE WITH SECTION 1-7.5-107(3), C.R.S., THE COUNTY CLERK AND RECORDER MUST MAIL BALLOTS NO LATER THAN 18 DAYS BEFORE THE ELECTION.

(A) THE COUNTY CLERK MUST PROCESS ALL NEW REGISTRATION APPLICATIONS AND UPDATES RECEIVED BY THE 22-DAY DEADLINE TO MAIL APPLICANTS A BALLOT IN ACCORDANCE WITH SECTION 1-7.5-107(3), C.R.S.

(B) THE COUNTY CLERK MUST PROCESS NEW ONLINE AND IN-PERSON REGISTRATION APPLICATIONS AND MAIL REGISTRATION UPDATES RECEIVED BY THE EIGHTH DAY BEFORE THE ELECTION AND MAIL A BALLOT WITHIN 24 HOURS AFTER THE APPLICATION IS SUBMITTED.

(C) IN COORDINATED ELECTIONS, THE COUNTY CLERK MUST MAIL BALLOTS TO ALL ACTIVE ELIGIBLE ELECTORS OF EACH POLITICAL SUBDIVISION. FOR SPECIAL DISTRICT ELECTIONS, THE DESIGNATED ELECTION OFFICIAL OF EACH DISTRICT MUST CERTIFY TO THE COUNTY CLERK THE LIST OF ELECTORS ELIGIBLE TO VOTE UNDER SECTION 32-1-806, C.R.S.

10.7.2.5 Voiding ballots due to timely changes in address or affiliation.

10.7.1(A) If an elector submits a timely changes his or her address or affiliation change after the county mails ballots or sends the voter file to the vendor, the county must void the first ballot and generate a second ballot.

(a)-(I) If the county processes the change to the elector’s record after it sends the voter file to the vendor but before the vendor prints ballots, the county must provide the vendor a voided ballot file to prevent the vendor from printing and preparing voided ballots for mailing.

(b)-(II) If the county processes the change to the elector’s record after the vendor has printed ballots but before the vendor mails ballots, the county must work with the vendor to make every reasonable effort to remove voided ballots before they enter the mail stream.
10.7.3 (b) If the county mails its own ballots, the county clerk must remove all voided ballots before mailing.

10.7.4 (c) If the county processes the change to the elector’s record after it mails ballots, the county must count the first ballot returned by the elector in accordance with section 1-7.5-107(6), C.R.S., except as follows:

(a) In the case of an affiliation change if the elector changed his or her affiliation, the county must count the ballot issued for the elector’s new party affiliation.

(b) In the case of an address change that results in a change of precinct, the county must count the ballot issued for the elector’s new address.

[Current Rule 10.7 is amended and moved to new Rule 7.2.5. Amendments are shown above.]

7.3 ABSENTEE VOTING

7.3.1 An elector may request that the county clerk mail his or her ballot to an address other than the elector’s address of record by submitting an application in accordance with section 1-7.5-116, C.R.S.

7.3.2 The county clerk must mail the ballot to the address provided until the elector indicates otherwise. Elector indicates otherwise.

7.4 EMERGENCY BALLOT TRANSMISSION

42.1.7.4.1 The county clerk and recorder may deliver a ballot to an elector’s authorized representative or to the elector by electronic transmission in the case of an administrative or medical emergency under section 1-7.5-115, C.R.S. If the county clerk delivers a mail-in ballot by facsimile-electronic transmission, the elector may return the ballot by facsimile-electronic transmission.

[Portions of current Rules 42.1 and 42.3 are included in new Rule 7.4.2.]

42.4.7.4.2 Mail-in ballots. Ballots sent by facsimile-electronic transmission shall must include all races, ballot issues, and questions on—for which the elector may be eligible to vote. Counties are encouraged to work with their vendors to develop a ballot that is clearly legible to the elector to increase the readability of the ballot and to avoid possible misinterpretations of the elector’s intended choice because of poor transmission of the document.

[Current Rule 42.4 is amended and moved to new Rule 7.4.3. Amendments are shown above.]

7.4.3 The ballot packet sent by electronic transmission must be in text
FORMAT ON 8 ½” X 11” WHITE PAPER AND MUST INCLUDE:

1. AN ELECTRONIC TRANSMISSION COVERSHEET TO PROTECT VOTER PRIVACY;
2. THE BLANK BALLOT;
3. THE ELECTRONIC TRANSMISSION BALLOT INSTRUCTIONS; AND
4. THE SELF-AFFIRMATION REQUIRED BY SECTION 1-7.5-107(3)(B.5), C.R.S.

7.4.4 THE ELECTRONIC TRANSMISSION MUST INCLUDE:

1. THE COUNTY CLERK AND RECORDER’S CONTACT INFORMATION INCLUDING MAILING ADDRESS, EMAIL ADDRESS, PHONE, AND FAX NUMBER;
2. A NOTICE THAT THE BALLOT MAY NOT BE DUPLICATED FOR ANY OTHER ELECTOR;
3. INSTRUCTIONS FOR COMPLETING AND RETURNING THE BALLOT;
4. A NOTICE REGARDING THE BALLOT RETURN DEADLINE;
5. INFORMATION REGARDING HOW THE ELECTOR MAY VERIFY THAT HIS OR HER BALLOT HAS BEEN RECEIVED BY THE COUNTY CLERK AND RECORDER; AND
6. ANY OTHER INFORMATION DEEMED NECESSARY BY THE SECRETARY OF STATE OR THE COUNTY CLERK AND RECORDER.

7.4.5 ANY BALLOT TRANSMITTED TO AN ELECTOR BY ELECTRONIC TRANSMISSION MUST CONTAIN A UNIQUE IDENTIFICATION NUMBER FOR TRACKING AND AUDITING PURPOSES.

7.4.6 THE COUNTY CLERK AND RECORDER MUST MAINTAIN A LOG OF EACH BALLOT SENT BY ELECTRONIC TRANSMISSION. THE COUNTY CLERK MUST RETAIN THE LOG AS PART OF THE OFFICIAL ELECTION RECORD ALONG WITH ANY OTHER ELECTRONIC TRANSMISSION RECORDS. THE LOG MUST INCLUDE:

1. THE NAME OF THE VOTER;
2. THE FAX NUMBER OR EMAIL ADDRESS TO WHICH THE BALLOT WAS TRANSMITTED (AS APPLICABLE);
3. THE UNIQUE IDENTIFICATION NUMBER OF THE BALLOT;
4. THE DATE THE BALLOT PACKET WAS TRANSMITTED; AND
5. THE INITIALS OF THE EMPLOYEE TRANSMITTING THE BALLOT.
42.8 7.4.7 The designated election official shall fax the blank ballot with the instructions to the fax number provided by the elector. If the COUNTY CLERK TRANSMITS A BALLOT PACKET TO AN ELECTOR BY FAX AND the transmission is unsuccessful, the designated election official shall—COUNTY CLERK MUST attempt to fax the BALLOT at least two more times and make reasonable effort, if possible, to ensure the transmission was successful.

[Current Rule 42.8 is amended and moved to new Rule 7.4.8. Amendments are shown above.]

42.9 7.4.8 Upon receipt of the ballot, THE COUNTY CLERK MUST VERIFY THE SIGNATURE ON THE AFFIDAVIT UNDER RULE 7.6. when the information from the signed—AFTER the affidavit has been verified, a bipartisan team of judges shall—MUST duplicate the ballot. Duplicating judges shall—MUST not reveal how the elector has cast his or her ballot.

[Current Rule 42.8 is amended and moved to new Rule 7.4.9. Amendments are shown above.]

7.5 RECEIPT AND PROCESSING OF BALLOTS

42.10.4 7.5.1 Monitoring drop-off locations—All drop-off locations must be monitored by an election judge or video security surveillance recording system, as defined in Rule 43.

(a) Freestanding drop-off locations must be monitored at all times.

(b) If the drop-off location utilizes a drop-slot into a building, the ballots must be collected in a locked container, and both the drop-slot and container must be monitored at all times.

[Current Rule 12.10.4 is amended and moved to new Rule 7.5.1. Amendments are shown above.]

42.7.2 7.5.2 Each day when ballots come in, a judge shall—MUST count the ballots, batch them and record the number of ballots received.

42.7.3 7.5.3 The ballots shall be date-stamped when received. An ELECTION JUDGE MUST DATE-STAMP AND RECEIVE THE BALLOTS INTO THE STATEWIDE VOTER REGISTRATION SYSTEM IMMEDIATELY UPON RECEIPT. If any ballot is received after the time set for the closing of the elections, the ballot shall—MUST be date-stamped but the ballot shall—NOT be counted. THE COUNTY CLERK MUST COLLECT BALLOTS FROM ALL DROP-OFF LOCATIONS, INCLUDING FREE STANDING BALLOT BOXES, HOURLY DURING REGULAR BUSINESS HOURS (INCLUDE OR MORE AS NEEDED?).
12.7.4 Records shall also be kept of the number of ballot packets returned as undeliverable.

12.7.5 Ballot packets shall then be placed in a safe, secure place until the counting of the ballots.

[Current Rule 12.7 is amended and moved to new Rule 7.5.2 through 7.5.5. Amendments are shown above.]

13.2 The county clerk and recorder shall keep a list, to the extent possible, of the names and mailing addresses of all individuals who deliver more than ten (10) voted mail-in ballots to the designated election official's COUNTY CLERK'S office, DROP-OFF LOCATION, OR VOTER SERVICE AND POLLING CENTER or the designated drop site for mail-in ballots.

[Current Rules 13.2 and 13.3 are amended and moved to new Rules 7.5.6 and 7.5.7. Amendments are shown above.]

10.9 Tracking ballot batches. The county clerk must dissociate any batch number that could trace a ballot back to the specific voter who cast it from the counted ballots no later than the final certification of the abstract of votes cast.

[Current Rule 10.9 is amended and moved to new Rule 7.5.8. Amendments are shown above.]

7.6 SIGNATURE VERIFICATION PROCEDURES

29.1 Missing Signature on Mail Ballot, Provisional Ballot or Mail-in Ballot Envelope

29.1.1 If a mail, mail-in, or provisional ballot return envelope lacks a signature, the election judge must contact the elector in writing no later than two calendar days after election day. The designated election official must use the letter and form prescribed by the Secretary of State and keep a copy as part of the official election record. Nothing in this rule prohibits the designated election official from calling the elector. But a phone call may not substitute for written contact. If the designated election official calls any elector he or she must call all electors whose affidavits are unsigned.

[Sections 1-7.5-107.3, 1-8-114.5, and 1-8.5-105(3)(a), C.R.S.]

29.1.2 The letter shall inform the eligible elector that he/she must come to the office of the county clerk and recorder to sign the mail ballot,
provisional ballot, or mail-in ballot envelope no later than eight calendar days after election day. The letter must inform military, overseas, and other electors who are absent from the state that they may sign the affidavit and return the form by mail, fax, or email, and that the county must receive the form no later than eight calendar days after the election.

29.1.3.7.6.3 The letter and missing signature affidavit form does not violate section 1-13-801, C.R.S.

29.1.4.7.6.4 The letter or missing signature affidavit form must include the following language:

“Any person who knowingly violates any of the provisions of the election code relative to the casting of ballots or who aids or abets fraud in connection with any vote cast, or to be cast, or attempted to be cast shall be punished by a fine of not more than five thousand dollars or by imprisonment in the county jail for not more than eighteen months, or by both such fine and imprisonment. Section 1-13-803, C.R.S.”

29.2.7.6.5 In accordance with section 1-8-114.5, C.R.S., for mail-in ballots and section 1-7.5-107.3, C.R.S., for mail ballots, the election judges shall. AN ELECTION JUDGE MUST compare the signature on the self-affirmation on each respective return envelope with the signature stored in the statewide voter registration system SCORE. Signatures shall require further research if any of the following discrepancies are discovered: THERE IS:

Code 1—(A) An obvious change in the slant of the signature

Code 2—(B) A printed signature on one document and a cursive signature on the other document

Code 3—(C) Differences A DIFFERENCE in the size or scale of the signature SIGNATURES

Code 4—(D) Differences A DIFFERENCE in the individual characteristics of the signatures, such as how the “t’s” are crossed, “i’s” are dotted, loops are made on “y’s” or “j’s”

Code 5—(E) Differences A DIFFERENCE in the voter’s signature style, such as how the letters are connected at the top and bottom

Code 6—(F) EVIDENCE THAT ballots or envelopes from the same household have been switched

Code 7—(G) ‘Other,’ ANY OTHER NOTICEABLE DISCREPANCY including misspelled names & description of discrepancy
29.3-7.6.6 If in conducting further research is necessary, the election judge shall
must check the county clerk’s or election official’s file SCORE for at least two
additional documents signed by the voter, if available. The judge may compare
additional information written by the voter on the return envelope, such as the voter’s
address and date of signing, may be compared for similarities. Any similarities noted
when comparing this other information may be used as part of the signature verification
decision process.

29.3-7.6.6 (A) If it appears to the judges verifying the self-affirmation on the return
envelopes that members of the same household who have applied for mail-in
ballots or have been sent mail ballots have inadvertently switched envelopes or
ballots, the ballot or ballots shall MUST be counted and no letter of advisement to
the elector is necessary.

29.4-7.6.7 Whenever If the election judge disputes the a signature is disputed, the
election judge shall the judge or she must document the discrepancy by completing
and the research steps taken in a log. The log shall provide a record of the research steps
taken to resolve the issue. The judge must identify the elector in the log will
identify the voter using a unique tracking number. This tracking number shall not contain the voter’s elector’s social security number; Colorado issued driver’s
license number, or the identification number issued by the Department of Revenue. The
log may not contain the elector’s signature. The judge must note the final
resolution and ballot disposition on the research log.

29.5–The log shall be approved by the Secretary of State pursuant to section 1-1-109, C.R.S.

29.6–There shall be no document containing the voter’s signature attached to the research log.

29.7–If both sets of election judges agree that the signatures do not match, the county clerk and
recorder shall within two days after the election, send a letter to the eligible elector at the
address indicated in the registration records and the address where the mail-in ballot or
mail ballot was mailed explaining the discrepancy in signatures and a form for the
eligible elector to confirm that the elector returned a ballot to the county clerk and
recorder. (Sections 1-7.5-107.3(2)(a) and 1-8-114.5(2)(a), C.R.S.) The voted ballot itself
should not under any circumstances be returned with this letter.

29.8-7.6.8 The election official must use the letter and the signature verification form
approved by the Secretary of State. (Sections 1-7.5-107.3(2)(a) and 1-8-114.5(2)(a),
C.R.S.) The letter and signature verification form does not violate section 1-13-801 C.R.S.

29.9–The letter and signature verification form does not violate section 1-13-801 C.R.S.

29.10–The final signature verification resolution and ballot disposition shall be noted on the
research log.

29.11-7.6.9 Any all uncounted ballot ballots shall must remain sealed in the return
envelope and stored under seal with all other uncounted ballots as part of the election
record pursuant to IN ACCORDANCE WITH section 1-7-802, C.R.S., and may be removed only under the authority of a district attorney or by order of a court having jurisdiction.

29.12 Use of Signature Verification Devices

29.12.1 7.6.10 A county clerk and recorder who chooses to use USES a signature verification device to process mail in or mail ballots in accordance with sections 1-7.5-107.3 or 1-8-114.5, C.R.S., shall MUST FIRST conduct acceptance testing on the device prior to its use in an election.

29.12.1 7.6.11 The acceptance testing conducted in accordance with this rule shall MUST be sufficient to verify the accuracy of the device. The acceptance testing shall AND MUST ensure that the device will not accept a signature that a reasonable, trained election judge would reject.

[Current Rule 29 is amended and moved to new Rule 7.6. Amendments are shown below.]

7.7 Voter Service and Polling Centers

7.7.1 The county clerk and recorder MUST designate and open the minimum number of voter service and polling centers and the locations MUST be open during reasonable business hours for the minimum number of days outlined in section 1-5-102.9, C.R.S., for a general election and 1-7.5-107(4.5), C.R.S., for all other elections.

(a) Reasonable business hours means at least eight hours per day Monday through Friday, and at least four hours on Saturday.

(b) All voter service and polling centers MUST be open from 7:00 AM through 7:00 PM on election day.

(c) The county clerk MUST provide all services outlined in section 1-2-509, C.R.S., at every designated voter service and polling center.

7.7.2 Polling place—Voter Service and Polling Center materials shall include, where applicable, sufficient computer stations for SCORE access, HAVA information, a voting demonstration display, a signature card table, registration records or lists, poll books, electronic or paper, or completed signature cards, paper ballots, and voting booths or DREs, provisional voting area or procedure, and a ballot box if provided.

[Current Rule 7.1 is amended and moved to new Rule 7.7.2. Amendments are shown above.]

7.7.3 Voter Check-in at the Voter Service and Polling Center

(a) Each voter service and polling center MUST include and
ADEQUATELY STAFF A DESIGNATED VOTER CHECK-IN TABLE OR AREA.

(B) THE CHECK-IN JUDGE MUST VERIFY EACH ELECTOR’S REGISTRATION INFORMATION, INCLUDING ADDRESS.

(C) IF AN ELECTOR HAS MOVED OR IS NOT REGISTERED, THE CHECK-IN JUDGE MUST DIRECT THE ELECTOR TO THE REGISTRATION AREA. IF THE ELECTOR IS REGISTERED AND HAS NO UPDATES, THE CHECK-IN JUDGE MUST DIRECT THE ELECTOR TO THE VOTING TABLE.

7.7.4 Except for voters with disabilities, the maximum allowable time in a voting booth is 15 minutes if there are voters waiting. The secretary of state may order additional time based on the length of the ballot. [Section 1-7-115, C.R.S.]

[Portions of current Rule 7.6 are included in new Rule 7.7.3.]

7.7.5 Any eligible elector may vote in-person at a voter service and polling center. The election judge must void the elector’s mail ballot before issuing an in-person ballot.

47.2-7.7.6 If a voter leaves the voting area without completing the voting process, two judges of different affiliation shall, to the extent possible, cover the voter’s choices, and cast the ballot as the voter left it.

[Current Rule 47.2 is amended and moved to new Rule 7.7.6. Amendments are shown above.]

7.7.7 Any individual who votes in an election for federal office as a result of a federal or state court issues an order extending or any other order that is in effect 10 days before that election and which extends the time established for closing the polls by state law, may only vote in that election by casting a provisional ballot pursuant to state law and the rules and regulations prescribed by the Secretary of State. The county clerk must keep all provisional ballots cast under this rule separate from provisional ballots not affected by the court order.

7.8 No later than 90 days before an election, the county clerk and recorder must designate drop-off locations and voter service and polling centers, and complete an accessibility survey for all voter service and polling center locations annually before designating a location for use.

7.8.1 For the first survey of a location, the county clerk must complete the full ADA checklist for polling places. The county clerk must complete the annual polling place accessibility survey form for each election after the initial survey is completed. [Section 1-5-102, C.R.S.]
7.7.2 Barrier removal: If, upon assessment, a location fails to meet the minimum accessibility requirements outlined in the ADA Checklist for Polling Places, the designated election official—COUNTY CLERK—must develop a barrier removal plan outlining the permanent and or temporary modifications that will be implemented. THE COUNTY CLERK WILL IMPLEMENT to bring the site into compliance in order for the location to be designated an official polling place location. THE COUNTY CLERK MUST INDICATE ON THE SURVEY WHETHER THE MODIFICATIONS ARE TEMPORARY OR PERMANENT.

[Current Rule 7.7.3 is amended and moved to new Rule 7.8.2. Amendments between the current and new rule language are shown above.]

7.8.3 THE SECRETARY OF STATE MAY DENY AN APPLICATION FOR ACCESSIBILITY GRANT FUNDS IF A COUNTY CLERK FAILS TO ASSESS LOCATIONS AND TIMELY FILE COMPLETE ACCESSIBILITY SURVEYS, AND DEVELOP AND IMPLEMENT NECESSARY BARRIER REMOVAL PLANS IN ACCORDANCE WITH THIS RULE. THE SECRETARY WILL CONDUCT SITE VISITS TO ASSESS COMPLIANCE AND IDENTIFY ACCESSIBILITY BARRIERS. THE SECRETARY WILL SEEK INJUNCTIVE ACTION OR OTHER PENALTIES UNDER SECTION 1-1-107(2)(d), C.R.S., AS NECESSARY TO REMEDY VIOLATIONS OF THIS RULE.

[Portions of current Rules 7.7.2(d) and 7.7.4 are included in new Rule 7.8.3.]

7.9 VOTER SERVICE AND POLLING CENTER CONNECTIVITY

7.9.1 THE COUNTY MUST HAVE REALTIME ACCESS TO THE STATEWIDE VOTER REGISTRATION SYSTEM AT EVERY VOTER SERVICE AND POLLING CENTER DESIGNATED BY THE COUNTY CLERK AND RECORDER.

7.9.2 AT NO TIME MAY AN ELECTION JUDGE OPEN BOTH THE SCORE VOTER REGISTRATION SCREEN AND THE VOTING MODULE ON A SINGLE WORKSTATION.

7.9.3 EVERY VOTER SERVICE AND POLLING CENTER DESIGNATED BY THE COUNTY CLERK AND RECORDER MUST MEET THE MINIMUM SECURITY PROCEDURES FOR TRANSMITTING VOTER REGISTRATION DATA AS OUTLINED IN SECTION 1-5-102.9, C.R.S., AND RULE 43.

7.10 ASSISTING VOTERS WITH DISABILITIES IN A VOTER SERVICE AND POLLING CENTER

9.1–7.10.1 The county clerk and recorder must post a sign at the polling place or voter center—VOTER SERVICE AND POLLING CENTER that states:

NOTICE

VOTING ASSISTANCE FOR ELECTORS WITH DISABILITIES

Colorado law protects a voter’s legal right to assistance in voting if assistance is needed
because of a disability.

1. If you require assistance, please inform an election judge.

2. Any person, including an election judge, may assist you.

3. If you select a person other than an election judge, he or she must complete a Voter Assistance Form, which includes an oath that states:

   I, ..........., certify that I am the individual chosen by the elector to assist the elector in casting a ballot.'

4. The person you select may provide any assistance you need, including entering the voting booth, preparing the ballot, or operating the voting machine.

5. The person assisting you may not seek to persuade you or induce you to vote in a particular manner.

6. The election judge must record the name of each voter who receives assistance and the name of the person who provides assistance in the pollbook or list of eligible electors (or on the signature card if preprinted signature cards are used in the place of a pollbook and list of eligible electors).

9.2-7.10.2 When a voter has spoiled two ballots and requests a third ballot, an election judge shall offer assistance in voting procedures and casting the ballot.

[Current Rule 9 is amended and moved to Rules 7.10. Amendments are shown above.]

Rule 8. Rules Concerning Watchers

8.2-8.1 Qualification of Watchers. Watchers shall certify that they are qualified pursuant to sections 1-1-104(51), 1-7-105, 1-7-106, 1-7-107, and 1-7-108(2), C.R.S., as applicable. Watchers shall take the oath as provided in section 1-7-108(1), C.R.S. and shall, upon first entering the precinct place, surrender the Certificate of Appointment to the election official or supervisor of voter service and polling center or location, where the watcher has been designated to act.

8.2-8.1.1 If a watcher leaves a precinct and the same watcher returns later in the day to the same location, another certificate of appointment is not necessary and shall not be required. The original certificate of appointment will suffice.

8.2-8.1.2 If a watcher is replaced during the day, the watcher replacing the original watcher must have an original certificate of appointment for that precinct. A new
WATCHE WHO IS REPLACING AN ORIGINAL WATCHER MUST PROVIDE AN ORIGINAL
CERTIFICATE OF APPOINTMENT FOR THAT VOTER SERVICE AND POLLING CENTER.

8.2.3-8.1.3 Certificate---A CERTIFICATE of appointment as a watcher is not transferable
to another individual.

8.3-8.2 A political party attorneys are not allowed in the polling place.
VOTER SERVICE AND POLLING CENTER unless they are HE OR SHE IS A duly appointed as
watcher--WATCHER.

8.4-8.3 Watchers are not allowed to have cell phones, cameras, recording devices, laptops or
PDAs (Palm Pilot, Blackberry, etc.) in the polling place. A WATCHER MAY NOT HAVE A
CELL PHONE, CAMERA, RECORDING DEVICE, COMPUTER, TABLET, OR OTHER PERSONAL
ELECTRONIC EQUIPMENT IN THE VOTER SERVICE AND POLLING CENTER.

8.5-8.4 List of Eligible Electors. To assist Watchers in performing their tasks, the election
official or election judge shall provide THE SUPERVISOR JUDGE MUST provide TO EACH WATCHER a
list, log, check-in card, or other similar information of voters who have appeared in the
precinct polling place--APPEARING IN THE VOTER SERVICE AND POLLING CENTER to vote.
The WATCHER MAY NOT REMOVE the information or documents shall not be removed
from the polling place or voting location FROM THE VOTER SERVICE AND POLLING CENTER.
Watchers---A WATCHER MAY maintain a list of eligible electors who have voted by utilizing
USING only that information provided by the election official or election judge except that they may bring with them into the polling place or location OR a list of
electors previously maintained by the watcher. [Section 1-7-108(3), C.R.S.]

[Current Rule 8.1 is moved to Rule 1. Current Rules 8.2, 8.3, 8.4, and 8.5 are amended
and moved to new Rules 8.1, 8.2, 8.3, and 8.4. Amendments are shown above.]

8.6-8.5 Watchers are subject to the provisions of section 1-5-503, C.R.S.

8.6.2-8.5.1 The designated election official must position the voting equipment,
voting booths, and the ballot box so that they are in plain view of the election
officials and watchers.

8.6.3-8.5.2 Watchers are permitted to A WATCHER MAY witness and verify the conduct
of elections and recount activities. Witness and verify means to personally
observe actions of election judges in each step of the conduct of an election.

(a) The conduct of election-ELECTIONS includes polling place and early voting
ALL ACTIVITIES IN A VOTER SERVICE AND POLLING CENTER and ballot
processing and counting.

(b) Watchers must remain outside the immediate voting area.

(c) Watchers may be present at each stage of the conduct of the election,
including the receiving and bundling of the ballots received by the
designated election official.
Watchers may be present during provisional ballot processing, signature verification, and UOCAVA ballot processing, but may not have access to confidential voter information.

The number of watchers permitted in any room at one time is subject to local safety codes.

Watchers—A WATCHER may witness and verify activities described in Article I, Article 1, Section 7, that are outside the immediate voting area, including ballot processing and counting. IF ELECTION OFFICIALS OR ELECTION JUDGES ARE CONDUCTING ELECTIONS ACTIVITIES IN SEPARATE ROOMS OR AREAS OF A BUILDING OR BUILDINGS, THE COUNTY CLERK AND RECORDER MUST ALLOW WATCHERS TO OBSERVE ACTIVITIES IN EACH ROOM OR AREA IN THE BUILDING OR BUILDINGS.

Watchers appointed under section 1-10.5-101(1)(a), C.R.S., THIS RULE 8 may observe the canvass board while it performs its duties.

Watchers—A WATCHER may track the names of electors who have cast ballots, challenge electors under section 1-9-203, C.R.S., and Rule 48, and submit written complaints in accordance with section 1-1.5-105, C.R.S., and Rule 31.8.7.

What Watchers May Observe. Duly appointed Watchers—A WATCHER may observe polling place voting, early voting, all activities in a voter service and polling center and the processing and counting of precinct, provisional, mail, and mail-in ballots. For mail ballot elections, or mail-in ballot processing, watchers—A WATCHER may be present at each stage of the election including the receiving and bundling of the ballots. received by the designated election official.

Watchers—A WATCHER may be present during provisional ballot processing but may not have access to confidential voter information.

Watcher oath. In addition to the oath required by section 1-7-108(1), C.R.S., a watcher must affirm that he or she will not:

Attempt to determine how any elector voted or review confidential voter information;

Disclose any confidential voter information that he or she may observe; or

Disclose any results before the polls are closed and the designated election official has formally announced results.

Limitations of Watchers. Watchers—A WATCHER may not:

Interrupt or disrupt the processing, verification and counting of any ballots or any other stage of the election.
8.8.2-8.7.2 Write down any ballot numbers or any other identifying information about the electors.

8.8.3-8.7.3 Handle the poll books, official signature cards, ballots, mail ballot envelopes, mail-in ballot envelopes, provisional ballot envelopes, voting or counting machines, or machine components.

8.8.4-8.7.4 Interfere with the orderly conduct of any election process, including issuance of ballots, receiving of ballots, and voting or counting of ballots.

8.8.5-8.7.5 Interact with election officials or election judges as defined in section 1-1-104(10) and (47), C.R.S., except for the individual designated by the election official.

8.9.1-8.8 A major and OR minor political parties—PARTY with candidates—A CANDIDATE on the ballot, OR A REGISTERED ISSUE COMMITTEE SUPPORTING OR OPPOSING A BALLOT MEASURE OR QUESTION ON THE BALLOT may appoint one Watcher each to be present OR MORE WATCHERS to observe polling place voting, early voting, and the processing and counting of regular, provisional, mail and mail-in ballots ELECTION ACTIVITIES. See [sections 1-7-105 and 1-7-106, C.R.S, AND RULE 8.6.4.]

[Current Rule 8.9.1 is amended and moved to rule 8.8. Amendments are shown above.]

8.10-8.9 Official Observers Appointed by the Federal Government. THE SECRETARY OF STATE MUST APPROVE Official Observers appointed by the federal government. shall be approved by the Secretary of State and shall be OFFICIAL OBSERVERS are subject to Colorado law and these rules as they apply to Watchers, however, they need not BUT AN OFFICIAL OBSERVER IS NOT REQUIRED TO BE AN eligible ELECTOR electors in the jurisdiction in which they act as Watchers. This Rule DOES not apply to Official Observers appointed by the United States Department of Justice. Official Observers appointed by the Secretary of State shall be ARE subject to the rules and regulations as prescribed by the Secretary of State. Official Observers shall MUST obtain a LETTER OF AUTHORITY from the Secretary of State, or his or her designee, duly executed letters of authority. The Official Observers shall MUST surrender such THE letter of authority to the COUNTY CLERK AND RECORDER designated election official in the jurisdiction in which they act as Watchers.

[Current Rule 8.10 is amended and moved to rule 8.9. Amendments are shown above.]

8.11-8.10 Watchers, Official Observers and Media Observers at a Recount. Watchers, Official Observers, and Media Observers may be present DURING a recount. Watchers, Official Observers, and Media Observers must be qualified and sworn IN for a recount in the same manner as provided AS DESCRIBED in Rule 8.2 and are subject to all other provisions related to the recount process. Any political party OR candidate involved in the recount or proponents or opponents of an issue or question involved in the recount may appoint one Watcher OR MORE WATCHERS to be present at any time during the recount. The A candidate who is subject to a recount may appoint him or her self HIMSELF OR HERSELF, or a member of the candidate’s family by blood, or marriage, OR CIVIL
UNION, as a watcher at a recount. See sections [SECTIONS 1-7-105 and 1-7-106, C.R.S., AND RULE 8.6.4.]

8.12-8.11 Media Observers.—Media Observers with valid and current media credentials may be present to witness early voting, election day voting and the processing and counting of provisional, mail and mail-in ballots—ALL ELECTION ACTIVITIES. However, at the discretion of the county clerk and recorder, Media Observers may be required. A COUNTY CLERK AND RECORDER MAY, IN HIS OR HER DISCRETION, REQUIRE A MEDIA OBSERVER to appoint one member of the media as a pool reporter and one member as a pool photographer to represent all media observers. ALL MEDIA OBSERVERS ARE SUBJECT TO in accordance with the Guidelines established by the Colorado Press Association in conjunction with the Colorado County Clerks’ Association and the Secretary of State as set forth herein OUTLINED BELOW:

Guidelines for Member of the Media Who Observe Election Counts and Recounts (to be distributed to members of the Colorado Press Association):

The Colorado State Association of County Clerks and Recorders, Colorado Broadcasters’ Association and Colorado Press Association have collaborated to develop the following guidelines and protocols for use when members of the media observe the counting or recounting of ballots. You are strongly encouraged to follow these guidelines to allow meaningful media access while not disrupting the work of county clerks to count ballots or doing anything to compromise the integrity of the election process.

1. If practical, please contact the election official’s office prior to coming to observe the counting of ballots. If the election official knows you are coming, it will be easier to accommodate your request for a place to observe the count or to interview an election official.

2. At the discretion of the election official, a specific viewing area for members of the media and other observers may be available. To the extent practicable, the area will have been designated with sight lines to allow you to observe and take pictures or video of the counting process. If there are insufficient sight lines for you to take the photos or video you need, the election official may be able to make arrangements to accommodate your needs.

3. Please observe counting procedures without disrupting the count. Please take pictures or video without the use of supplemental lighting. Do not talk to people participating in counting ballots. There may be workers who ask you not to include their images in your pictures or video. We encourage you to honor those requests if you can reasonably do so.

4. The Secretary of State’s election rules state that if observers leave the area during a recount, they may not reenter without the consent of the
election official. If you have occasion to leave the area, you may be denied re-admittance.

5. Please do not use the information you see when observing vote counts to report on partial election results. Please do not report anything that could be used to identify the person who casts a particular ballot.

The Colorado State Association of County Clerks and Recorders, Colorado Broadcasters’ Association and Colorado Press Association are all committed to working together to ensure the media has access to election counts and recounts, but that access is afforded in manners that do not disrupt the counts and do nothing to compromise the integrity of the process. Your cooperation in following these standards will help us to meet all these goals.

[Current Rules 8.11 and 8.12 are amended and moved to new Rules 8.10 and 8.11. Amendments are shown above.]

8.13-8.12 Watchers at Vote Centers. To assist Watchers in performing their tasks when a vote center election is held at a voter service and polling center, the designated election official shall provide a list of all voters who have voted in the location appeared in the vote centers to vote. This list shall be made available at the designated election official’s main office. The clerk may make the such list may be made available to a requesting Watcher(s) in the form of data files, paper, or reports, and furnished to all interested parties via email, paper reports, or faxed copies as may be available to the designated election official.

8.14-8.13 A designated election official shall the county clerk must certify the appointment of all eligible watchers duly designated by a political party, candidate or committee pursuant to sections 1-1-104(51), 1-7-105, 1-7-106, or 1-7-107, C.R.S.


8.15.1-8.14.1 A designated election official county clerk may remove a watcher upon finding that the watcher:

(a) Commits or encourages fraud in connection with his or her duties;

(b) Violates any of the limitations outlined in Rule 8.8;

(c) Violates his or her oath;

(d) Is abusive or threatening toward election officials or voters.

8.15.2-8.14.2 Upon removal of a watcher, the designated election official county clerk must inform the political party, candidate, or committee who appointed the watcher.
8.14.3 A removed watcher may be replaced by an alternate watcher duly designated in accordance with sections 1-7-105, 1-7-106, or 1-7-107, C.R.S. Any designated election official—COUNTY CLERK who removes a watcher must, to the best of the official’s ability, expeditiously certify the appointment.

8.15.3 Watchers may be designated to observe more than one precinct or polling place, but in no event shall more than one watcher be designated for any single polling place. See section 1-7-106, C.R.S.

8.16 Watchers may be appointed to observe recall elections held pursuant to UNDER article 12, title I, C.R.S., and shall MUST be designated in accordance with sections 1-7-106 and 1-7-107, C.R.S.

[Current Rules 8.13, 8.14, 8.15, 8.16 and 8.17 are amended and moved to new Rules 8.10 and 8.11. Amendments are shown above.]

Rule 9. Voting Challenges

48.19.1 Under Section 1-9-201, C.R.S., an election judge, poll watcher, or eligible elector of the precinct may challenge an elector’s right to vote. Pursuant to section 1-9-203 (7), C.R.S., a person whose eligibility is challenged must be offered a regular ballot by the election judge when if the person challenged satisfactorily answers the applicable challenge questions specified in section 1-9-203(3)(a)-(e), C.R.S. The following demonstrate when a person challenged satisfactorily answered the challenge questions and action to be taken by the election judge based on the elector’s response: If the person challenged provides unsatisfactory answers or refuses to answer the challenge questions, an election judge must offer the person a provisional ballot.

9.2 Citizenship

A. Are you a citizen of the United States?

Satisfactory Answer: Yes.

IF THE PERSON CHALLENGED ANSWERS YES, AN ELECTION JUDGE MUST OFFER THE PERSON A REGULAR BALLOT.

 Unsatisfactory Answer: No.

IF THE PERSON CHALLENGED ANSWERS NO, AN ELECTION JUDGE MUST OFFER THE PERSON A PROVISIONAL BALLOT.

9.3 Residency

A. Have you resided in this state and precinct COLORADO for the past thirty 22 days immediately preceding this election?
Satisfactory response—ANSWER: Yes, he/she has resided in this state—COLORADO and precinct for the entire thirty—22-day period immediately preceding this election. (In other words, his/her primary home or place of abode was in this state—COLORADO and precinct during the entire thirty—22-day period in accordance with sections 1-1-104(43) and 1-2-102, C.R.S.)

*IF THE PERSON CHALLENGED ANSWERS YES, Proceed continue to challenge question B.*

Unsatisfactory response—ANSWER: No, for some portion of the thirty-22-day period immediately preceding this election, he/she has not resided in this state—COLORADO and precinct.

*IF THE PERSON CHALLENGED ANSWERS NO, THE ELECTION JUDGE MUST CONTINUE TO CHALLENGE QUESTION B. Offer the elector a provisional ballot.*

B. IF YOU HAVE BEEN absent from this state—COLORADO during the past thirty-22 days immediately preceding this election, DID YOU AND during that time have you maintained a home or domicile elsewhere?

Satisfactory response #1 ANSWER: No, he/she either has not been absent from this state at any time COLORADO during the thirty—22-day period immediately preceding this election: OR HAS BEEN ABSENT BUT HAS NOT MAINTAINED A HOME OR DOMICILE ELSEWHERE.

*IF THE PERSON CHALLENGED ANSWERS NO, Offer THE ELECTION JUDGE MUST OFFER the elector PERSON a regular ballot.*

Satisfactory response #2: Yes, he/she has been absent from this state during the thirty-day period immediately preceding this election, but has not maintained a home or domicile elsewhere.

Offer the elector a regular ballot.

UNSATISFACTORY Response requiring follow-up questions—ANSWER: Yes, he/she has been absent from this state—COLORADO during the thirty—22-day period immediately preceding this election, and has maintained a home or domicile elsewhere.

*IF THE PERSON CHALLENGED ANSWERS YES, THE ELECTION JUDGE MUST Proceed continue to challenge question C.*

C. HAVE YOU BEEN ABSENT if so, when you left, was it for a temporary purpose with the intent of returning, or did you intend to remain away OUTSIDE COLORADO?

Satisfactory response—ANSWER: Yes, when he/she left, it was for a temporary purpose with the intent of returning.
IF THE PERSON CHALLENGED ANSWERS YES, THE ELECTION JUDGE MUST Proceed CONTINUE to challenge question D.

Unsatisfactory response—ANSWER: No, when he/she left, he/she did not intend to return.

IF THE PERSON CHALLENGED ANSWERS NO, THE ELECTION JUDGE MUST Offer OFFER the elector person a provisional ballot.

D. Did you, while YOU WERE absent, DID YOU look upon and regard CONSIDER this state as COLORADO TO BE your home?

Satisfactory response—ANSWER: Yes, while absent, he/she looked upon and regarded this state as COLORADO TO BE his/her home.

IF THE PERSON CHALLENGED ANSWERED YES, Proceed CONTINUE to challenge question E.

Unsatisfactory response—ANSWER: No, while absent, he/she did not LOOK UPON AND REGARD this state as COLORADO TO BE his/her home.

IF THE PERSON CHALLENGED ANSWERS NO, THE ELECTION JUDGE MUST Offer OFFER the elector-PERSON a provisional ballot.

E. Did you, while YOU WERE absent, DID YOU vote in any other state or any territory of the United States?

Satisfactory response—ANSWER: No, while absent, he/she did not vote in any other state or any territory of the United States.

The election judge must Offer—OFFER the elector-PERSON a regular ballot.

Unsatisfactory response—ANSWER: Yes, while absent, he/she did vote VOTED in another state or territory of the United States.

The election judge must Offer—OFFER the elector-PERSON a provisional ballot.

9.4 AGE

A. WILL YOU BE 18 YEARS OF AGE OR OLDER ON ELECTION DAY?

Satisfactory answer: YES.

IF THE PERSON CHALLENGED ANSWERS YES, AN ELECTION JUDGE MUST OFFER THE PERSON A REGULAR BALLOT.

Unsatisfactory answer: NO.
IF THE PERSON CHALLENGED ANSWERS NO, AN ELECTION JUDGE MUST OFFER THE PERSON A PROVISIONAL BALLOT.

48.2—If the person challenged answers unsatisfactorily or refuses to answer the challenge questions, the elector shall be offered a provisional ballot.

[Current Rule 48 is amended and moved to Rule 9. Amendments are shown below.]

Rule 10. CANVASSING AND RECOUNT

41.1—Definitions

41.1.1 “Canvass board” means a committee composed of the county clerk and recorder and the registered electors appointed by the major parties in accordance with section 1-10-101, C.R.S.

41.1.2 “Canvass workers” means workers appointed or hired by the designated election official to assist in the preparation and conduct of the canvass.

41.1.3 “Statement of Ballots Form” means the form used at the polling location that accounts for all ballots at that location and includes all information required by this rule.

[Current Rule 41.1 is moved to new Rule 1]

41.2—10.1 Appointment to the Canvass Board

41.2.1 10.1.1 In all cases, the canvass board must consist of an odd number of members, and each member has equal voting rights.

41.2.2 10.1.2 For a partisan election, each major party may have no more than two representatives on the canvass board. The board must include an equal number of representatives from each major party, unless a major party fails to certify representatives for appointment.

41.2.3 10.1.3 Each major party representative on the canvass board must be registered to vote in the county where the representative will serve and affiliated with the party he or she represents.

41.2.4 10.1.4 A candidate for office and members of the candidate’s immediate family may not serve on the canvass board.

41.3—10.2 Duties of the Canvass Board

41.3.1 10.2.1 The canvass board must make its determinations by majority vote in accordance with section 1-10-101.5(3), C.R.S.

41.3.2 10.2.2 The canvass board’s duties are:
(a) Conduct the canvass in accordance with section 1-10.5-101, C.R.S., including:

(i) Account and balance the election and certify the official abstract of votes;

(i) Reconcile the number of ballots counted to the number of ballots cast; and

(iii) Reconcile the number of ballots cast to the number of voters who voted by reviewing the reconciled detailed ballot logs and Statement of Ballots;

(b) Observe the post-election audit in accordance with section 1-7-514(4), C.R.S., and Election Rule 11.5.4;

(c) In coordination with the county clerk and recorder, investigate and report discrepancies found in the audit under section 1-7-514(2), C.R.S.; and

(d) Conduct any recount in accordance with section 1-10.5-107, C.R.S., and Election Rule 14. The canvass board’s role in conducting a recount includes selecting ballots for the random test, observing the recounting of ballots, and certifying the results.

41.3.3 10.2.3 If the board identifies a discrepancy in the Statement of Ballots, the Board may review the particular ballots at issue to identify, correct, and account for the error.

41.3.4 10.2.4 The canvass board may not perform duties typically reserved for election judges, including:

(a) Determining voter intent;

(b) evaluating voter eligibility; and

(c) Requesting new logs or reports that were not created to conduct the election.

41.4 10.3 Detailed Ballot Log

41.4.1 10.3.1 The designated election official must keep a detailed ballot log that accounts for every ballot issued and received beginning when ballots are ordered and received. The election judges must reconcile the log at the conclusion of each workday.

41.4.2 10.3.2 The designated election official must keep and reconcile daily logs of mail-in, mail, and early voting ballots.

41.4.3 10.3.3 The designated election official must indicate in the detailed log the
number of paper ballots that are sent to each polling location for use on election
day.

41.4.4 The designated election official must keep required logs in either
electronic or manual format.

41.5 Election Day Tracking Process

41.5.1 The designated election official must supply each polling location with a
Statement of Ballots Form. Combined precincts may use one form. The form
must include a place for the judges to account for the following information:

(a) The name or number(s) of the precinct or vote center;

(b) The number of ballots provided to the polling location;

(c) The number of ballots cast;

(d) The number of unvoted ballots;

(e) The number of damaged or spoiled ballots; and

(f) The number of voted provisional ballots.

41.5.2 The election judge must reconcile the total number of voted ballots with
the number of voters who voted.

41.5.3 The election judge must verify that the total number of voted ballots,
spoiled or damaged ballots, provisional ballots, and unvoted ballots is the same
as the number of total ballots supplied to the polling location.

41.5.4 The election judge must reconcile the number of people who signed the
pollbook to the total of the number of ballots cast.

41.5.5 If there is a discrepancy in the numbers on the Statement of Ballots form,
the judge must explain the discrepancy in writing (for example, the voter signed
in but left the polling place without voting, etc.).

41.5.6 The judge must return the completed Statement of Ballots form to the
designated election official with the other precinct supplies and mail a duplicate
copy to the designated election official’s office.

41.6 Designated Election Official’s Disposition of Forms

41.6.1 The designated election official must review the Statement of Ballots form
for completion and accuracy.

41.6.2 If the designated election official or the canvass board discovers a problem
with the Statement of Ballots form that cannot be easily resolved, they may
contact the election judges for an explanation or correction.

41.7.10.6 Procedures for the Day of the Canvass

The designated election official must provide the following information to the canvass board:

(a) The name of each candidate, office, and votes received;

(b) The number/letter of each ballot issue or question and votes received;

(c) The number of voters who voted early;

(d) The number of mail-in or mail ballots cast, including the number accepted and rejected; and

(e) The number of provisional ballots counted.

41.7.2 10.6.2 Any written documentation regarding official numbers is included as part of the canvass.

41.8 10.7 Official Abstract

41.8.1 10.7.1 The designated election official must include the number of eligible voters on election day on the official abstract.

41.8.2 10.7.2 The canvass board must use the official abstract in a format approved by the Secretary of State.

41.8.3 10.7.3 The official abstract must include, by precinct/ballot style or vote center, where applicable:

(a) The statement of votes counted by race and ballot question or issue;

(b) The total active registered electors in the precinct and the total for the jurisdiction holding the election;

(c) The total number of electors voting in each precinct and the total for the jurisdiction holding the election;

(d) The number of voters who voted early;

(e) The number of emergency registrations;

(f) The number of mail-in or mail ballots counted and the number rejected;

(g) The number of provisional ballots counted and the number rejected listed by each rejection code; and
(h) The number of damaged and spoiled ballots.

41.9 10.8 The Abstract is the Official Permanent Record.

41.9.1 10.8.1 The designated election official must keep all official canvass reports and forms as part of the official permanent election record.

41.9.2 10.8.2 Once the canvass board certifies the abstract it may not withdraw the certification. In the event of a recount, the canvass board may only affirm or amend the abstract.

41.10 10.9 Appointment of Canvass Workers.

41.10.1 The designated election official may appoint canvass workers to help prepare and conduct the canvass.

41.11 10.10 Voter History.

41.11.1 10.10.1 After the canvass, the designated election official must give credit to each voter who votes by mail, at an early voting site, or at a polling location.

41.11.2 10.10.2 If the voter history records do not match the number of voters who voted at that election, the designated election official must ensure the following:

(a) Each voter received credit for voting; and

(b) All pollbooks and signature cards are accounted for.

41.11.3 10.10.3 All research concerning discrepancies must be explained and documented.

41.12 10.11 Written Complaints.

41.12.1 10.11.1 The designated election official must provide the canvass board with any written complaint submitted by a registered elector about a voting device.

41.12.2 10.11.2 If the complaint is resolved, the designated election official must provide the details of the resolution

41.12.3 10.11.3 If the complaint is pending resolution when the board meets to conduct the canvass, the designated election official must provide a proposal for how the issue will be resolved.

41.13 10.12 Role of Watchers.

41.13.1 10.12.1 Watchers appointed under section 1-10.5-101(1)(a), C.R.S., may observe the board while it performs its duties, subject to Rule 8.
41.14 10.13 Role of the Secretary of State.

10.13.1 As part of the Secretary’s duties under section 1-1-107, C.R.S., the Secretary may provide guidance and investigate imperfections as outlined below.

41.14 10.13.2 The county clerk and recorder or the canvass board may request that the Secretary of State provide guidance and support to the canvass board in the exercise of the board’s duties.

41.14 10.13.3 If, in the course of assisting a canvass board, the Secretary of State discovers an imperfection that the Secretary believes may affect the conduct of other canvass boards, the Secretary may provide notice to other counties regarding the nature of the imperfection.

41.14 10.13.4 Imperfect returns or failure to certify.

(a) If the canvass board fails to certify or certifies imperfect returns that have no reasonable potential to change the outcome of any race or ballot measure, the Secretary of State and county clerk must certify the election and order recounts, if any, in accordance with Part 1, Article 11 of Title 1, C.R.S.

(b) If the canvass board fails to certify or certifies imperfect returns that have a reasonable potential to change the outcome of any race or ballot measure, the Secretary of State will conduct an investigation to identify the nature of, and advise the county clerk and recorder in correcting, the inaccuracy.

[Current Rule 41 moved to new Rule 10 Amendments between the current and new rule language are shown above.]

44.3 10.14 Recount Generally.

10.14.1 The purpose of a recount is to RE-TABULATE THE BALLOTS—review the ballots to assure they were counted properly. Unless directed otherwise by the Secretary of State, all procedures of election night shall be followed as closely as possible during the recount, including an examination of the ballots.

10.14.2 FOR STATEWIDE OR FEDERAL RACES, BALLOT ISSUES OR BALLOT QUESTIONS, THE COUNTY CLERK AND RECORDER MUST COORDINATE SCHEDULING THE RECOUNT THROUGH THE SECRETARY OF STATE’S OFFICE SO THAT IT CAN ENSURE ADEQUATE OBSERVER COVERAGE.

10.15 Recount Cost Estimates and Reimbursements

10.15.1 A COUNTY MUST SUBMIT A REQUEST FOR REIMBURSEMENT FOR A MANDATORY RECOUNT IN A STATEWIDE OR FEDERAL RACE USING THE SECRETARY OF STATE
APPROVED FORM. THE COUNTY MAY NOT REQUEST REIMBURSEMENT FOR MEALS
OR NORMAL OVERHEAD COSTS OR REGULAR EMPLOYEE COMPENSATION. THE
COUNTY MUST INCLUDE ITEMIZED COSTS FOR REASONABLE EXPENDITURES,
INCLUDING:

(A) MAILINGS AND NOTICES;

(B) ELECTION JUDGES, TEMPORARY STAFF, CANVASS BOARD PAY, AND
OVERTIME PAY; AND

(C) COPIES AND OTHER OFFICE EXPENSES RELATED TO THE RECOUNT.

10.15.2 REQUESTED RECOUNTS

(A) THE COUNTY CLERK MUST PROVIDE A COST ESTIMATE IN ACCORDANCE
WITH SECTION 1-10.5-106, C.R.S., UPON SUBMISSION OF A FORMAL
REQUEST FOR A RECOUNT.

(B) IN PREPARING A COST ESTIMATE FOR A REQUESTED RECOUNT, THE COUNTY
MUST USE THE SECRETARY OF STATE APPROVED FORM. THE ESTIMATE MUST
INCLUDE REASONABLE ITEMIZED COSTS FOR CONDUCTING THE RECOUNT.
THE COUNTY MAY NOT REQUEST REIMBURSEMENT FOR NORMAL OVERHEAD
COSTS.

(C) ANY OTHER COSTS AGREED TO BY THE REQUESTING PARTY.

(D) THE COUNTY CLERK MUST SUBMIT A COST ESTIMATE TO THE SECRETARY OF
STATE WHEN THE CLERK PROVIDES IT TO A REQUESTING PARTY.

10.16 IN ACCORDANCE WITH SECTION 1-10.5-107, C.R.S., AND RULE 10.2.2(d), THE CANVASS
BOARD’S ROLE IN CONDUCTING A RECOUNT INCLUDES SELECTING BALLOTS FOR THE TEST,
OBSERVING THE RECOUNTING OF BALLOTS, AND CERTIFYING THE RESULTS.

14.4.10.17 General Provisions. WATCHERS AND OBSERVERS

14.4.1 10.17.1 The Secretary of State may have appoint an official observer at every
recount location in any recount.

14.4.2 Any candidate who is subject to the recount may be present and observe the
recount at any recount location or designate one watcher to observe the recount
at any recount location. Watchers must provide the election official with a
certificate signed by the candidate, except that an officer of the county party
may be accepted as a candidate’s watcher without a certificate if no other person
is designated by the candidate for that location.

14.4.3 10.17.2 Each candidate, his or her watcher, or the candidate’s watcher,
members of the media observers, and official observers as defined in Rule 8.1,
may be present in the room when a...
ACCORDANCE WITH RULE 8. During the recount, the candidate, watcher, members of the media, and official observers may not interfere with the recount process.

10.17.3 The recount board, candidates, AND watchers, members of the media, and official observers will MUST take an oath.

10.17.4 COMPLAINTS. A WATCHER MAY SUBMIT A COMPLAINT IN WRITING TO THE COUNTY CLERK. WRITTEN COMPLAINTS DURING A RECOUNT WILL BE ADDRESSED IN ACCORDANCE WITH RULE 4

10.18 Testing

10.18.1 THE CANVASS BOARD MUST REVIEW THE POST-ELECTION AUDIT BEFORE SELECTING THE EQUIPMENT FOR TESTING UNDER SECTION 1-10.5-102, C.R.S. TO THE EXTENT FEASIBLE, THE BOARD MUST SELECT EQUIPMENT FOR TESTING THAT WAS NOT INCLUDED IN THE POST-ELECTION AUDIT.

10.18.2 THE COUNTY CLERK MUST TEST ALL SCANNERS THAT WILL BE USED IN THE RECOUNT. THE PURPOSE OF THE TEST IS TO ENSURE THAT THE TABULATION MACHINES ARE COUNTING PROPERLY.

(A) THE TEST DECK MUST INCLUDE 50 BALLOTS OR 1% OF THE TOTAL NUMBER OF BALLOTS CAST IN THE ELECTION, WHICHERVER IS GREATER, EXCEPT THAT THE TOTAL NUMBER OF BALLOTS TESTED MAY NOT EXCEED THE TOTAL NUMBER OF BALLOTS TESTED IN THE LOGIC AND ACCURACY TEST BEFORE THE ELECTION. THE BALLOTS MUST BE MARKED TO TEST EVERY OPTION FOR THE RACE OR MEASURE THAT WILL BE RECOUNTED

(1) IN A MANDATORY RECOUNT, THE CANVASS BOARD MUST SELECT THE BALLOTS TO BE TESTED FROM THE PRE-ELECTION PUBLIC LOGIC AND ACCURACY TEST DECK.

(2) IN A REQUESTED RECOUNT, THE PERSON REQUESTING THE RECOUNT MAY MARK UP TO 25 BALLOTS. ANY OTHER CANDIDATE IN THE RACE MAY ALSO MARK UP TO 25 BALLOTS. THE CANVASS BOARD MUST RANDOMLY SELECT BALLOTS FROM THE PRE-ELECTION PUBLIC LOGIC AND ACCURACY TEST DECK TO ENSURE THE MINIMUM NUMBER OF TEST BALLOTS REQUIRED BY THIS RULE.

(B) SWORN JUDGES OR STAFF MUST HAND TALLY THE TEST BALLOTS FOR COMPARISON TO THE TABULATION RESULTS.

(C) THE TEST IS LIMITED TO THE RACE OR MEASURE THAT IS RECOUNTED.

10.18.3 THE COUNTY CLERK MUST TEST THE VVPAT RECORDS FROM 1% OF THE DREs THAT HAD VOTES CAST FOR THE RACE OR MEASURE BEING RECOUNTED.
1. (A) Sworn judges or staff must manually verify the results on the machines selected for the test.

2. (B) The test is limited to the race or measure that is recounted.

10.19 Counting of ballots

10.19.1 In accordance with section 1-10.5-102(3)(b), C.R.S., if there are no discrepancies in the test under Rule 14.6, the recount must be conducted in the same manner as the ballots were counted in the election except as outlined in this rule.

14.6.5 10.19.2 A clear audit trail must be maintained throughout the recount including, but not limited to, a log of seal numbers on transfer cases or ballot boxes as defined in section 1-7-505, C.R.S., and the corresponding numbered seal used as a replacement for the original seal, upon completion of the recount of ballots within that FOR EACH transfer case or ballot box.

[Current Rule 14.6.5 is amended and moved to new Rule 10.19.2. Amendments between the current and new rule language are shown above.]

10.19.3 Ballots must be reviewed for voter intent using the standards in Rule 18.

18. (A) Every ballot with an over-vote or under-vote in the race(s) or measure(s) subject to the recount must be reviewed for voter intent using the same guidelines that were used during the election.

22. (B) The judges conducting the voter intent review may resolve the intent differently than the judges in the election.

10.19.4 To recount ballots on optical scanners:

25. (A) If the original count method was central count, the county must create a new election database.

28. (B) If the original count was by precinct count, the county must use one or more blank PROM cartridges, ROM cartridges, or memory cards.

30. (C) All precinct ballots may be tabulated centrally regardless of whether precinct or central tabulation was used on election day.


10.19.5 Ballots for the recount shall be processed following the State of Colorado
Procedures for the use of the Ballot Now Voting System in conjunction with the following procedures: TO RECOUNT BALLOTS USING “BALLOT NOW”:

(A) BACK UP THE OFFICIAL ELECTION DATABASE.

(aB) Open Ballot Now with an unused MBB (Mobile Ballot Box) from the election and create a Ballot Now recount database.

(bc) Scan and resolve all recount ballots following original election procedures ACCORDING TO THIS RULE 14.

(e) Use the Audit Trail Report and Original Scan Batch Reports with notes to ensure that resolution action follows the original resolution.

(d) Save all recount CVRs (Cast Vote Records) to the MBBs (Mobile Ballot Box) after verifying that the number of ballots processed matches the number of ballots cast in the recount contest(s).

(e) Open a new recount election in “Tally” and process the recount MBBs following the tabulation procedures above.

(f) Compare recount results to original results and document any differences.

(g) Backup the test database and the official recount database following the “Archive” procedures.

[Portions of current Rule 14.7.1 and 14.7.2 are moved to Rule 10.19.5. Current Rule 14.7.3 is amended and moved to new Rules 10.19.5. Amendments are shown above.]

10.19.6 TO RECOUNT BALLOTS BY HAND COUNT.

(A) IF THE TABULATION OF THE ORIGINAL COUNT WAS CONDUCTED BY HAND COUNT, THE RECOUNT MUST BE CONDUCTED BY HAND COUNT.

14.5.4 (B) Ballots shall MUST be counted into groups in batches of 25 to ensure that the number of ballots recounted matches the number originally counted.

14.5.5 (C) Votes shall MUST be counted by individual hash marks in 25-count sections by two different judges.

[Current Rules 14.5.4 and 14.5.5 are amended and moved to new Rules 10.19.6(a) and (b). Amendments between the current and new rule language are shown above.]

10.19.7 FOR TABULATION OF DREs, IF THERE ARE NO DISCREPANCIES IN THE TEST UNDER RULE 14.6, THE COUNTY CLERK MUST UPLOAD THE MEMORY CARDS.
10.19.8 Tabulation of ballots cast by one method must be completed through a precise, controlled process that ensures each container of ballots is recounted, resealed, and retabulated before tabulation of the next method begins. Except that, if mail-in ballots were originally counted with early voting ballots, the recount must be conducted in the same manner.

10.19.9 The number of ballots counted by a method and precinct according to the election night report shall be final results for that race or measure must be available during the recount for comparison purposes.

[Current Rule 14.6.6 moved to new Rule 10.19.9. Amendments between the current and new rule language are shown above.]

14.6.7 10.20.1 Totals of recounted ballots shall be processed, counted, and reported in summary form as follows:

(a) Sum total of votes cast for each candidate, ballot issue or ballot question subject to the recount—race or measure recounted, under-votes, and over-votes for all precincts;

(b) Sum total of votes cast for each candidate, ballot issue or ballot question subject to the recount—race or measure recounted, under-votes and over-votes for all mail-in ballots (a combined total, not totaled by individual precincts or location, unless your system allows);

(c) Sum total of votes cast for each candidate, ballot issue or ballot question, subject to the recount—race or measure recounted, under-votes, and over-votes for all early voting locations (a combined total, not totaled by individual precinct or locations, unless the voting system so allows);

(d) Determine the grand total of ballots cast in early, mail-in, and precinct voting.

(e) The totals must be a combined total, not totaled by individual precincts or location, unless the tabulation system allows.

[Current Rules 14.5.1 and 14.6.7 are amended and moved to new Rule 10.20.1. Amendments are shown above.]

10.20.2 In accordance with section 1-10.5-107, C.R.S., and this Rule 10, the canvass board must amend, if necessary, and re-submit the abstract of votes cast.

Rule 11. Rules Concerning Voting Systems
11.1 Voting system access.

11.2.1 The county clerk and recorder shall not program or operate the voting system subject to section 15-607, C.R.S.

11.2.2 11.1.1 Any election setup materials shall be stored by The county clerk and recorder MUST SECURELY STORE ELECTION SETUP RECORDS under security with access limited to the person or persons so authorized in writing by the county clerk and recorder. NO PERSON MAY ACCESS THE RECORDS WITHOUT THE CLERK’S WRITTEN AUTHORIZATION.

11.2.3 11.1.2 Employees of the county clerk and recorder who are authorized by the county clerk and recorder to prepare or maintain the voting system or election setup materials shall RECORDS MUST BE DEPUTIZED BY THE COUNTY CLERK AND RECORDER for this specific purpose and so sworn prior to BEFORE the first election of the calendar year in which they will be performing one or more of these activities.

11.2.4 11.1.3 The county clerk and recorder shall request an Internet Criminal History Check (ICHC) from the Colorado Bureau of Investigation (CBI) for all full-time, part-time, permanent and contract employees of the county who staff the counting center and OR who have any access to the electromechanical voting systems or electronic vote tabulating equipment. At the direction of the county clerk and recorder, an ICHC check may be conducted on election judges. The county clerk and recorder shall request the ICHC once per calendar year for such employees prior to the first election of the year. IN ACCORDANCE WITH SECTION 24-72-305.6, C.R.S., ALL PERMANENT AND TEMPORARY COUNTY STAFF AND ALL VENDOR STAFF WHO HAVE ACCESS TO THE VOTING SYSTEM OR ANY VOTING OR COUNTING EQUIPMENT MUST PASS THE CRIMINAL BACKGROUND CHECK DESCRIBED IN RULE 6.4.

11.2.5 If the ICHC indicated that the employee or contract employee has been found guilty of a crime involving breach of trust, fraudulent, coercive, or dishonest practices or demonstrating incompetence, untrustworthiness, or election offenses pursuant to sections 1-13-101 et seq., C.R.S., the county clerk and recorder shall MUST PROHIBIT SUCH EMPLOYEE OR CONTACT EMPLOYEE FROM PREPARING, PROGRAMMING, OPERATING, USING OR HAVING ANY ACCESS WHATSOEVER TO ELECTROMECHANICAL VOTING SYSTEMS OR ELECTRONIC VOTE TABULATING EQUIPMENT AT ANY TIME DURING THAT PERSON’S EMPLOYMENT.

11.2.6 Vendors or their authorized representatives shall provide a criminal history check to the county clerk and recorder for any employee of the vendor who has any access to electromechanical voting systems or electronic vote tabulating equipment. The vendor shall provide the criminal history check ICHC to the county clerk and recorder once per calendar year for such employees prior to the first election of the year.
11.2 Performance Bond.

11.2.1 Effective upon the date of the adoption of this rule, a voting system provider or service provider that provides election setup or tabulation services to one or more counties shall MUST:

(a) Provide the services by ENTER INTO A written contract, AND FILE a copy of which shall be kept on file with the county clerk and recorder and the Secretary of State.

(b) Post a performance bond, executed by a corporate surety licensed to transact business in the State of Colorado. The county under contractual obligation with the voting system provider or service provider that provides election setup or tabulation services shall MUST be designated as the NAMED beneficiary of the bond; and. THE BOND AMOUNT MUST BE THE GREATER OF $10,000 OR THE FULL AMOUNT OF THE CONTRACT WITH THE BENEFICIARY COUNTY AND THE BOND MUST BE ON FILE 30 DAYS BEFORE WORK STARTS.

(c) Provide proof that a OF THE performance bond has been posted with TO the Secretary of State and the office of the designated election official COUNTY CLERK AND RECORDER. The amount of the bond shall be the greater of either $10,000 or the full amount of the contract with the beneficiary county.

11.3.2 Performance bonds shall be on file 30 (thirty) days prior to any work commencing under contract with the county.

11.2.3 The voting system provider shall MUST update all bond documents for each contract or election. performed.

11.3.4 Copies of the performance bond for the secretary of state’s office shall be sent to: Colorado Department of State, Voting Systems Specialist, 1700 Broadway, Suite 270, Denver, Colorado 80290, or to voting.systems@sos.state.co.us

11.3 Voting System Inventory.

11.3.1 The designated election official shall MUST maintain an inventory record for each electronic vote-tabulating device used in an election. Such records shall THE RECORD MUST include, but not be IS NOT limited to, the manufacturer, make, model, serial number, hardware/firmware/software version or release number, hash value documentation where applicable, date of acquisition, description of any services, repairs, maintenance, upkeep, and version upgrades, and the dates of performance of such services as of the date of adoption of these rules THE SERVICES WERE PERFORMED.

11.3.2 IF THE INVENTORY IS IN ELECTRONIC FORMAT, IT MUST BE EXPORTABLE TO A COMMA SEPARATED (CSV), EXCEL SPREADSHEET (XLS OR XLSX), OR QUOTE OR
The designated election official shall furnish the inventory with the Secretary of State with an extract or copy of the inventory no later than 10 days before the election for use in the Logic and Accuracy Test and the Post-Election Audit Test. The requirements for this extract are:

(a) Be in either electronic or paper format;

(b) Contain information regarding: make, model, serial number, type (optical scanner or DRE), and specific location of use, and specific precincts programmed on each device or card;

(c) Inventories maintained in electronic format shall be exportable to an industry standard file type — comma separated (CSV), excel spreadsheet (XLS or XLSX), or Quote or Tab separated (TXT) file prior to electronic delivery to the Secretary of State; and

(d) The designated election official shall send the inventory list to the Secretary of State’s office not less than ten (10) days prior to an election to the attention of the Voting Systems Specialist. Inventory lists may be sent by mail, e-mail, or fax, in one of three means: E-mail: voting.systems@sos.state.co.us Subject line = County Number, County Name, HARDWARE INVENTORY LIST; or Via facsimile to: 303-869-4861 attn: Secretary of State, Voting Systems Specialist; or via First Class Mail to Colorado Department of State/Attn: Voting Systems Specialist/1700 Broadway—Suite 270/Denver, CO 80290.

11.4 Voting System Testing.

11.5.1 The clerk must perform a hardware diagnostic test, a logic and accuracy test, and a post-election audit test. Three types of voting system testing: shall be performed for each election within a jurisdiction. The three tests are:

- A Hardware Diagnostic Test;

- A Logic and Accuracy Test (LAT); and

- A Post-Election Audit Test.

11.5.2 11.4.1 Hardware Diagnostic Test

(a) The county clerk and recorder shall commence the Hardware Diagnostic Test prior to the election on each device that the clerk will use in the election, including spare or back up devices. The test must include the
FOLLOWING DEVICES AND PROVIDE THE FOLLOWING INFORMATION:
and allow time for each electronic voting device within the county

to be tested. Each device being used in the election, including units
identified as spare or backup units, shall be tested to verify that
mechanical components are working correctly. This test shall
include, but not be limited to, the following tests:

(a) (1) All input and output devices;

(b) (2) Communications ports;

(e) (3) System printers;

(d) (4) System modems when applicable;

(e) (5) System screen displays;

(f) (6) Boot performance and initializations;

(g) (7) Firmware loads;

(h) (8) Software loads;

(i) (9) Display of firmware OR software hash value (MD5 or SHA-
1) when possible;

(j) (10) Confirmation that screen displays are functioning; and

(k) (11) Date, time and calibration of systems.

11.5.2.2 (b) THE CLERK MUST SEAL each device tested shall be sealed upon the
successful completion of the test AND RETAIN documentation of the
seal information and all records from testing must be maintained
for each device IN ACCORDANCE WITH SECTION 1-7-802, C.R.S.

11.5.3 11.4.2 Logic and Accuracy Test. The designated election official shall conduct a
Logic and Accuracy Test according to the following requirements.

11.5.3.1 (a) The designated election official shall MUST create a Testing Board
consisting of at least two persons one registered elector
affiliated with the major political parties, as defined in
section 1-1-104(22), C.R.S., and one registered elector from
each other major political party, if appointed. Testing board
members must be registered to vote in the county.

11.5.3.2 (b) Prior to the commencement of voting, The designated election
official shall MUST conduct the public Logic and Accuracy Test
BEFORE VOTING.
11.5.3.3 (c) The DESIGNATED ELECTION OFFICIAL MUST ENSURE THAT THE Logic and Accuracy Test shall be IS open to representatives of the press and THE MEDIA AND the public to the extent allowable and pursuant to IN ACCORDANCE WITH section 1-7-509(2)(b), C.R.S. The designated election official may limit the number of representatives from each group to accommodate for BECAUSE OF space limitations and OR other considerations.

11.5.3.4 (d) Testing Board Test Ballots—In preparation for the Logic and Accuracy Test, The designated election official shall MUST provide to each member of the Testing Board, at least twenty-five (25) CLEARLY-MARKED TEST ballots that are clearly marked as test ballots TO EACH TESTING BOARD MEMBER to be used for the Logic and Accuracy Test.

11.5.3.5 (e) The members of the Testing Board MEMBERS shall MUST secretly vote their position BALLOTS IN ACCORDANCE WITH THE INSTRUCTIONS PRINTED ON THE BALLOTS and retain a record of the tally. of their test votes. The test ballots shall MUST have a known predetermined outcome by the members of the Testing Board’s secret vote and tally. Of the twenty-five 25 test ballots, two shall MUST be tested as audio ballots where applicable.

11.5.3.6 (f) County Test Ballots—In preparation for the Logic and Accuracy Test, The designated election official shall MUST prepare a sufficient number of test ballots that represent every precinct which shall INCLUDE AND every ballot style, allow for a sufficient number of ballots to mark every vote position for every candidate on every race including write-in candidates, allow for situations WHERE APPLICABLE, and include overvotes and undervotes for each race.

11.5.3.7 (g) The test ballots shall TESTING BOARD MUST be tested TEST THE BALLOTS on each type of voting device utilized USED in a given THE election and each method of counting. TYPE OF BALLOT INCLUDING The tests shall include testing of mail ballot counting methods, election-day counting methods, early voting counting methods and audio ballots, if applicable.

11.5.3.8 (h) Conducting the Test.

11.5.3.8.1 (1) The designated election official and Testing Board shall MUST observe the tabulation of all test ballots by means of the voting device and compare the tabulation with the previously retained records of the test vote count.
of AND MUST CORRECT any discrepancies shall be corrected prior to the start of BEFORE vote tabulation.

11.5.3.8.2 (2) Prior to the start of testing, THE DESIGNATED ELECTION OFFICIAL MUST all devices used will have the public counter reset THE PUBLIC COUNTER to zero ON ALL DEVICES, and PRESENT ZERO TAPES presented to the Testing Board for verification. For any device capable of producing OR VERIFYING the trusted build hash value (MD5 or SHA-1) of the firmware or software, the DESIGNATED Election Official shall MUST verify and document the accuracy of the value to be included with the records for the device.

11.5.3.8.3 (3) THE DESIGNATED ELECTION OFFICIAL MUST MAKE an appropriate number of voting devices will be available and the Testing Board may witness the necessary programming and/or downloading of memory devices necessary to FOR THE test. the specific precincts.

11.5.3.8.4 (4) The Testing Board and designated election official or his or her designated deputized clerks, as necessary, shall MUST count the test ballots as follows:

(a) Mail-in Ballots:

(1) All county test ballots shall be counted on at least one, but not more than three, mail-in ballot vote counting devices and have the predetermined total verified to the machine total.

(2) All Testing Board Member test ballots shall be counted individually with reports generated to verify the machine count to the predetermined hand tally:

(b) Precinct Count Ballots (Optical Scan and DRE):

(1) The Testing Board shall randomly select 20% but not more than 10 ballots representing unique precincts from the Testing Board’s test ballots.

(2) In the event a selected precinct contains a combination of DRE and Optical Scan voting devices, the Testing Board shall decide on the percentage of ballots to be counted on each type of device used for that precinct.
(3) The precinct-specific county test ballots will be added to the testing board test ballots to be counted on the specific precinct device. The testing board shall manually verify the ballots to be counted prior to any machine count.

(4) The Testing Board shall verify the manual count to the voting device count.

(e) (A) Vote Center Count Ballots—Optical Scan Scanners:

(1) All testing board The Testing Board test ballots shall MUST be counted COUNT TEST BALLOTS on at least one, but not more than 5 FIVE voting devices, WHICH MUST REPRESENT AT LEAST ONE DEVICE USED AT A VOTER SERVICE AND POLLING CENTER, AND ONE CENTRAL COUNT DEVICE designated for Vote Center Counting and have the predetermined total verified to the machine total.

(II) THE TESTING BOARD MUST RANDOMLY SELECT THE MACHINES TO TEST.

(2) (III) All The Testing Board must count the board’s AND THE COUNTY’S test ballots BALLOT BATCHES shall be counted individually SEPARATELY AND GENERATE REPORTS with reports generated to verify THAT the machine count IS IDENTICAL to the predetermined tally of the test ballots.

(3) The testing board shall randomly select the machines to be tested.

(d) (B) Vote Center Count Ballots—DREs:

(1) (I) All testing board THE TESTING BOARD MUST COUNT the test ballots shall be counted on at least one, but not more than 5 FIVE DREs. designated for Vote Center Counting and have the predetermined total verified to the machine total.

(II) THE TESTING BOARD MUST RANDOMLY SELECT THE MACHINES TO TEST.

(III) THE TESTING BOARD MUST IDENTIFY AND TEST TWO BALLOTS AS AUDIO BALLOTS.
(2) (iv) All the Testing Board must count the board’s and the county’s test ballots individually separately and generate reports with reports generated to verify that the machine count is identical to the predetermined tally of the test ballots. For DREs with VVPAT devices, the Testing Board must manually count the paper record to verify that the pre-determined totals of the Testing Board and county test ballot batches match the VVPAT total.

(3) The testing board shall randomly select the machines to be tested.

(e) Early Voting and Provisional Ballots Counted on Optical Scan Devices:

(1) All test ballots shall be counted on at least one, but not more than five, optical scan devices designated for Early Voting or Provisional Ballot Counting and have the predetermined total verified to the machine total.

(2) All test ballots shall be counted individually with reports generated to verify the machine count to the predetermined tally of the test ballots.

(f) Early Voting and Provisional Ballots Counted on DREs:

(1) All test ballots shall be counted on at least one, but not more than five, DREs designated for Early Voting or Provisional Ballot Counting and have the predetermined total verified to the machine total.

(2) All Testing Board Member test ballots shall be counted individually with reports generated to verify the machine count to the predetermined tally of the Testing Board test ballots.

11.5.3.8.5 DREs equipped with VVPAT devices shall be manually verified (by hand) to determine that the pre-determined total of the testing board ballots, matches the V-VPAT total, which in turn matches the machine total.

11.5.3.8.6 At least two of the testing board ballots shall be identified as Audio Ballots to be tested as such, and included with the count.
11.5.3.8.7  (5) The designated election official must keep all test materials, when not in use, shall be kept in a metal durable, secure box with individual seals for each member of the Testing Board. The designated election official may affix his or her own seal in addition to those of the Testing Board. The designated election official shall must be the custodian of the box or boxes but shall may not open and/or use the test materials outside of the Testing Board’s presence.

(6) After testing, the Testing Board must watch the designated election official reset and seal each voting device.

11.5.3.8.8  (7) The Testing Board and the designated election official shall must sign a written statement attesting to the qualification of each device that was successfully tested, the number of the seal attached to the voting device at the end of the test, any problems discovered, and provide any other documentation as necessary to provide a full and accurate account of the condition of a given device.

11.5.3.8.9  Upon completion of the testing, the Testing Board shall witness the resetting and sealing of each tested voting device.

11.5.4  11.4.3 Post-Election Audit

11.5.4.1  (a) Within forty-eight (48) no later than 48 hours after the close of polls on election night, the Secretary of State shall must notify the designated election official which voting devices and which race or races on the ballots have been selected for auditing purposes will be audited based on the submitted hardware inventory list referred to in Rule 11.4.2.

11.5.4.2  (b) The selection of Secretary of State will randomly select equipment will be based on a random selection of five (5) percent of precinct count scanners, scanner-based voting equipment, at least one central count scanner/vote center, and five (5) percent of Direct Record Electronic (DRE) DRE voting devices.

11.5.4.3  (c) Pursuant to in accordance with section 1-7-514, C.R.S., the Secretary of State may only select devices used in the election. shall be selected for the audit.

(d) The Secretary of State must randomly select at least two races per device for verification to ensure that each race or measure on the ballot is audited in accordance with section 1-7-514, C.R.S.
11.5.4.4 For optical scanners used for any function of counting ballots except for Central Count/vote center as defined herein, the designated election official shall manually verify all of the ballots that were counted on the randomly selected device(s) with the election summary report that was generated from the device(s) at the close of the polls. The Secretary of State shall randomly select a minimum of two (2) races per device to be manually verified to ensure that each office, issue, and question on the ballot is audited in accordance with section 1-7-514, C.R.S.

11.5.4.5 (e) For optical scanners used for the purpose of counting ballots in a Central Count/vote center environment as defined herein, the designated election official shall randomly select either of the following amounts based upon the total number of ballots counted:

1. If less than 500 ballots were counted, then a minimum of 20 percent of the ballots counted on the device.

2. If 500 or more ballots were counted, then a minimum of 100 ballots plus five (5) percent of the difference between the number of ballots counted and 500, but not more than 500. Five hundred (500) ballots of all the ballots counted on the specific audited device. If the amount of ballots is less than five hundred (500) on the audited device, then a minimum of twenty percent (20%) of the ballots counted on the device will be manually verified.

(f) The designated election official must reset the public counter for that voting device. The voting device shall be reset to zero and recounted the ballots.

(g) The designated election official must manually verify the new report will be generated from the electronic count. of the ballots and shall be manually verified.

(h) The designated election official must seal the ballots and a copy of the report shall be sealed in a separate container, and secured with the remainder of the official election records for the election. The Secretary of State shall randomly select a minimum of two (2) races per device to be manually verified to ensure that each office, issue, and question on the ballot is audited in accordance with section 1-7-514, C.R.S.

11.5.4.6 (i) For Direct Record Electronic Devices (DREs) DREs that do not meet the requirements of section 1-5-802, C.R.S. WITHOUT A VVPAT, used for any function of counting ballots in an election,
the designated election official will **MUST** manually verify the image of all the ballots contained in the **Ballot Log** or **Ballot Audit** that were counted on the specific device counted along with the report generated for that specific device at the close of polls, which contains the election summary report. The Secretary of State shall randomly select a minimum of two (2) races per device to be manually verified to ensure that each office, issue, and question on the ballot is audited in accordance with section 1-7-514, C.R.S.

11.5.4.6.4 (1) For any device capable of producing OR VERIFYING the trusted build hash value (MD5 or SHA-1) of the firmware or software, the designated election official **MUST** verify and document the accuracy of the value to be included with the records for the device prior to conducting the audit.

11.5.4.7 (j) For Direct Electronic Devices (DREs) that **WITH A VVPAT** do meet the requirement of section 1-5-802, C.R.S., used for any function of counting ballots in an election, after the close of the polls, the designated election official **MUST** manually verify all of the entire voter verified paper VVPAT record produced with the report generated for that specific device, which contains the election summary report. The Secretary of State shall randomly select a minimum of two races on each device to be manually verified to ensure that each office, issue, and question on the ballot is audited in accordance with section 1-7-514, C.R.S.

11.5.4.7.4 (1) For any device capable of producing OR VERIFYING the trusted build hash value (MD5 or SHA-1) of the firmware or software, the designated election official **MUST** verify and document the accuracy of the value to be included with the records for the device prior to conducting the audit.

11.5.4.8 (k) **AT LEAST TWO CANVASS BOARD MEMBERS MUST OBSERVE** the actions of the random audit as identified in this section are to be observed by at least two members of the canvass board. The designated election official may appoint additional deputized clerks to assist **WITH** in the functions of the audit.

11.5.4.9 (l) If there are discrepancies in the audit, the Canvass Board or the designated election official’s deputized clerks shall **OFFICIAL MUST:**

11.5.4.9.1 (1) **First, manually verify the results as many times as necessary to Confirm that there is no discrepancy in the manual count;**
11.5.4.9.2 (2) Second, take any additional steps as necessary to check for voter error, which shall MUST include but IS not be limited to: overvotes, stray marks on the ballot, or other voter intent indicia; and

11.5.4.9.3 (3) Third, review the situation and Take ANY action as necessary in accordance with the Canvass Board’s powers as set forth DESCRIBED in part 1 of Article 10 of Title 1, Colorado Revised Statutes.

11.5.4.10 (m) At all times relevant to the Post-Election DURING THE audit, the designated election official or the deputized clerks or the Canvass Board shall MUST take every precaution necessary to protect the confidentiality of the CAST ballots cast by the electors.

11.5.4.11 (n) Upon completion of AFTER the audit, the designated election official shall MUST promptly report the results of the audit to the Secretary of State’s Office by 5:00 PM ON THE LAST DAY TO CANVASS. The report shall MUST be submitted following the completion of the audit and up to and including 5:00 pm on the last day of the canvass. The report shall MUST contain:

(a) (1) The make, model, and serial number of the voting device DEVICES that was audited;

(b) (2) The number of ballots originally counted by the EACH device or the number of ballots audited as identified in paragraph (d) (4) of this section;

(c) (3) The count of the specific race or races as provided on the summary report printed at the close of polls or the report generated for the audit;

(d) (4) The count of the specific race RACES as manually verified;

(e) (5) Any other information required by section 1-7-514, C.R.S.; and

(f) (6) The signature CANVASS BOARD MEMBERS’ AND DESIGNATED ELECTION OFFICIAL’S SIGNATURES of the canvass board and the designated election official.

11.5.4.12 (o) The DESIGNATED ELECTION OFFICIAL MAY SEND the report may be sent by REGULAR MAIL, E-MAIL, OR FAX, any of the following three methods: E-mail: voting.systems@sos.state.co.us; Subject line = County Number, County Name, POST-ELECTION AUDIT; or via facsimile to: 303-869-4861 attn: Secretary of State, Voting Systems Specialist; or via First Class Mail: to Colorado
11.6 Procedures for Voter-Verifiable Paper Audit Trail (V-VPAT)

11.6.1 Security

11.6.1.1 The V-VPAT record is considered an official record of the election, pursuant to section 1-5.802. All security procedures related to election ballots shall apply to V-VPAT records.

11.6.1.2 The housing unit for any V-VPAT record to be used in the election shall be sealed and secured prior to any votes being cast for the election. Documentation of the seal number(s) must be maintained and noted prior to voting, and at the conclusion of voting.

(a) Election Judges shall attest to the V-VPAT record having no votes included on the paper record prior to the start of voting, and prior to the installation or replacement of a new V-VPAT record.

11.6.1.3 If a DRE with V-VPAT is used during early voting, the seal number(s) must be recorded at the beginning and end of each voting day.

11.6.1.4 At the Close of the polls, the V-VPAT records will be transferred to the central office in the same manner as any paper ballots. In the absence of paper ballots, the V-VPAT records will be transferred to the central office in the same manner as any memory cards containing electronic ballots.

11.6.2 Anonymity

11.6.2.1 The Election Official shall put measures in place to protect the anonymity of voters choosing to vote on DREs during the voting periods. These measures shall include:

(a) Encouraging poll workers to personally vote on DREs when possible to ensure more than one vote will be cast on the device.

(b) Appropriate marking in Poll Book or other voting list indicating voters choice to vote on DRE with the words: “Voted DRE”, or similar in place of paper ballot information. No record shall be kept indicating the order in which people voted on the DRE, or which V-VPAT record is associated with the voter.
(c) When more than one DRE is available at a voting location, the voter shall be given the choice as to which DRE they would like to vote on, to the extent practical.

(d) Encouraging or allowing any and all voters the opportunity to vote on a DRE if desired.

11.6.2.2 Any report or export (electronic or paper-based) generated from an Electronic Pollbook shall remove the date/time stamp from the record and not use this field as a sort method. Any assignment of Record IDs, Key ID, or Serial Number stored in the database of votes shall be randomly assigned.

11.6.2.3 Any Pollbook, electronic, paper or otherwise shall not be exposed to the same people at the same place who have exposure to the V-VPAT records.

11.6.2.4 The examination of the V-VPAT record shall always be done by at least two witnesses.

11.6.3 Storage

11.6.3.1 The storage of the V-VPAT records must be consistent with storage of Paper Ballots pursuant to section 17-802.

11.6.3.2 Individual spools containing V-VPAT records must contain the following catalog information affixed to the spool:

(a) Date and Name of Election;

(b) Name of Voting Location;

(c) Date(s) and Time(s) of Voting;

(d) Machine Serial Number of DRE Associated with the Record; and

(e) Number of spools associated with this machine for this election (i.e. “Spool 1 of 1”, or “Spool 1 of 2”, etc.).

11.6.3.3 Light-sensitive storage containers shall be used for the 25-month storage period to ensure the integrity of the V-VPAT paper record. Containers shall be sealed, with record of the seal numbers maintained on file and signed by two elections officials.

11.6.3.4 A master catalog shall be maintained for the election containing the complete total number of V-VPAT spools used in the election.
11.7 11.5 Escrow of County Election Setup. The designated election official must submit election setup records by regular mail no later than 5:00 PM on the seventh day before an election.

11.7.1 No later than 5:00 pm on the seventh (7th) day prior to any election, the designated election official shall deposit a copy of the election setup records with the Secretary of State’s office by mail.

11.7.2 Jurisdictions that have contracted with either a Software Service Bureau or a Vendor of Electronic Vote Counting Equipment may choose to have the Vendor deliver the necessary election setup records. delivered to the Secretary of State’s office within the specified time frame.

11.7.3 Election Setup Records shall be contained within an electronic media format that is native to the jurisdiction’s specific ballot creation and tabulation system. Acceptable media formats include Tape, Diskette, Cartridge, CD-ROM, DVD-ROM, Floppy, External Hard Drive, or Flash Media.

11.7.4 All copies of electronic media shall be sent to:

Colorado Secretary of State
Attn: Voting Systems Specialist
1700 Broadway—Suite 270
Denver, CO 80202

11.7.5 Jurisdictions will include a point of contact and method of contact (phone, fax, e-mail, etc.) to inform the jurisdiction that the Secretary of State’s office has received the election setup records.

11.7.6 Within 24 hours of receipt of the election setup files, the Secretary of State or his or her designee will contact the jurisdiction to confirm receipt of the escrow files.

11.7.7 The Secretary of State’s office will store the election setup files in a secured, fire proof, limited-access location or container.

11.7.8 All parties shall treat as confidential all escrowed materials and any other related information that comes into their possession, control, or custody, pursuant to this rule.

[Rule 11.8 is amended and moved to New Rule 45.12]
11.8.1 Voting System Providers must place in escrow a copy of the election software and supporting documentation being certified with either the Secretary of State or an independent escrow agent approved by the Secretary of State. See section 1-7-511, C.R.S.

11.8.2 Within ten days of the Voting System provider receiving notification of examination of voting equipment as part of the certification process, the Voting System Provider shall arrange for the completion of escrow requirements as indicated by this rule.

11.8.3 Voting System Provider shall sign a sworn affidavit that the election software in escrow is the same as the election software used in its voting systems in this state. An annual update of the affidavit will be on file in a secured location with the Secretary of State’s office.

11.8.4 A complete copy of the certified election software including any and all subsystems of the certified software shall be maintained in escrow.

11.8.5 Any changes to current configurations or new installations must be approved through the certification program of the Secretary of State.

11.8.6 In addition to the requirements listed below, the Voting System Provider must include a cover/instructions sheet for any escrow material to include the Voting System Provider Name, Address and pertinent contact information, Software Version, Hardware Version, Firmware Revision Number and other uniquely identifying numbers of the software submitted for certification.

11.8.7 Election Software Source Code, maintained in escrow, shall contain internal documentation such that a person reasonably proficient in the use of the programming language can efficiently use the documentation to understand the program structure, control techniques, and error-processing logic in order to maintain the Source Code should it be removed from escrow for any reason.

11.8.8 System documentation shall include instructions for converting the escrowed Source Code into Object Code, organized and configured to produce an executable system, if warranted.

11.8.9 System documentation shall include technical architecture design, analysis, detail design, testing and an installation and configuration guide.

11.8.10 A set of schematics and drawings on electronic vote casting and counting equipment purchased or in use by the county clerk and recorder shall be on file with the Secretary of State.

11.8.11 All parties shall treat as confidential the terms of this Section including all escrow materials and any other related information that comes into their possession, control or custody pursuant to this section.
11.8.12 Copies of Electronic media and supporting documentation for Escrow within the Secretary of State shall be sent to:

Colorado Secretary of State  
Attn: Voting Systems Specialist  
1700 Broadway—Suite 270  
Denver, CO 80290  

11.8.13 Any cost of using an alternative third party escrow agent shall be borne by the Voting System provider.

11.6 THE DESIGNATED ELECTION OFFICIAL MUST RETAIN ALL TESTING RECORDS AND DOCUMENTATION FOR 25 MONTHS.

11.7 METHODS OF SUBMISSION ARE:

11.7.1 BY REGULAR MAIL TO:

COLORADO SECRETARY OF STATE  
ATTN: VOTING SYSTEMS  
1700 BROADWAY—SUITE 200  
DENVER, CO 80290  

11.7.2 BY EMAIL TO:  
VOTING.SYSTEMS@SOS.STATE.CO.US  

11.7.3 BY FAX TO:  
303-869-4861  

11.8 RULES CONCERNING ACCESSIBLE VOTING SYSTEMS

34.2 11.8.2 No political subdivision shall MAY NOT purchase or lease direct recording electronic DRE voting systems or other voting systems equipped for individuals USE BY PEOPLE with disabilities at each polling place unless such voting system(s) THEY are fully certified pursuant to standards and guidelines recommended by the National Institute of Standards and Testing (NIST) and adopted by the U.S. Election Assistance Commission (EAC) IN ACCORDANCE WITH THE 2002 VOTING SYSTEM STANDARDS PROMULGATED BY THE FEDERAL ELECTION COMMISSION.

[Rule 34 is amended and moved to New Rule 11.9. (Amendments are shown above)]

11.9 RULES CONCERNING NOTICE OF VOTING SYSTEM MALFUNCTION

36.1 11.9.1 A vendor or the political subdivision DESIGNATED ELECTION OFFICIAL if no private vendor supports their system must give notice to NOTIFY the Secretary of State within 24 hours of a REPORTED OR ACTUAL malfunction of its voting/election system (including, but not limited to, software, firmware, hardware, or other equipment) in preparation for and on an
election held in this state. The notice must include a description, date, and the names of those who witnessed the malfunction, as well as the procedures followed prior to the malfunction, and any error messages displayed. The notice may be verbal, but must also be in a writing must follow.

36.2 Following the notice, the Secretary of State shall determine whether further information on the malfunction is required. At the request of the Secretary of State, a vendor (or the political subdivision, if no private vendor supports their system) must submit a report to the Secretary of State’s office detailing the reprogramming (or any other actions) necessary to correct a voting system malfunction in preparation for and on an election held using the vendor’s system. The report shall address whether permanent changes are necessary to prevent similar malfunctions in the future. If the malfunction requires a programming or election setup change to the database or other parts of the voting system, the designated election official shall submit an updated electronic copy of the election system database to the Secretary of State’s office as set forth in Rule 11.

11.9.2 If the Secretary of State requires additional information the vendor or the designated election official must submit a report to the Secretary of State’s office detailing the reprogramming or any other actions necessary to correct a voting system malfunction.

(A) The report must address whether permanent changes are necessary to prevent similar malfunctions in the future.

(B) If the malfunction requires a programming or election setup change to the database or other parts of the voting system, the designated election official must submit an updated election setup record to the Secretary of State’s office as set forth in Rule 11.8.

36.3 (C) The report shall must be submitted within 30 days after the date of the request by the Secretary of State. Notwithstanding the foregoing, if an election is scheduled within 60 days of the date of request by the Secretary of State, the Secretary of State may set an emergency deadline for filing the report. The request may be verbal, but must also be in writing.

36.4 (D) Failure to submit a report within the required period shall be grounds to decertify the system.

36.5 (E) The political subdivision holding the election in which the voting system malfunction occurred may submit the report in lieu of a report from the system’s vendor.

36.6 (F) A copy of this report will be attached to the system’s most recent certification on file in the Secretary of State’s office.
36.7 (G) The Secretary of State's office will distribute a copy of this report to all counties using the voting system in question.

[Rule 36 is amended and moved to New Rule 11.10. Amendments are shown above]

11.10 PURCHASES AND CONTRACTS

11.10.1 IN ACCORDANCE WITH SECTION 1-5-623(3), C.R.S., A POLITICAL SUBDIVISION MAY NOT PURCHASE A NEW ELECTRONIC VOTING DEVICE OR SYSTEM OR ANY RELATED COMPONENT OF A DEVICE OR SYSTEM WITHOUT APPROVAL FROM THE SECRETARY OF STATE.

45.12.1 11.10.2 Any A POLITICAL SUBDIVISION MAY ONLY PURCHASE OR LEASE A CERTIFIED voting system for that has been certified under the procedures of Rule 45 are is eligible for purchase, lease, or rent for use by jurisdictions within the State of Colorado providing if the contract contains the following items:

(a) The voting system is certified for use within the state;

(b) (A) The contract contains training and maintenance costs for the jurisdiction; and

(e) (B) The contract identifies components contained in the certified THE voting system COMPONENTS and appears complete with all accessories necessary APPEAR COMPLETE AND CAPABLE OF for successfully conducting an election within the laws and rules of the State of Colorado.

45.12.2 11.10.3 The Secretary of State shall WILL maintain on file a list of all components used and purchased for use. The list shall will include, at a minimum, the name of the jurisdiction, the date of purchase, the serial number(s) of voting devices and name of the voting systems that was were purchased.

[Rule 45.12 is amended and moved to New Rule 11.11. Amendments are shown above]

11.11 ELECTION NIGHT REPORTING (ENR). THE COUNTY MUST REPORT ELECTION NIGHT RESULTS FOR ALL PRIMARY, GENERAL, COORDINATED AND RECALL ELECTIONS.

11.11.1 A DATA ENTRY COUNTY MUST PROGRAM THE ELECTION TO SUPPORT THE EXPORTING OF ELECTION NIGHT RESULTS IN ACCORDANCE WITH THE FOLLOWING ENR VENDOR’S DATA UPLOAD REQUIREMENTS:

(A) LIST CONTEST NAMES AND CANDIDATE NAMES EXACTLY AS PROVIDED ON THE CERTIFIED LIST.

(B) PROVIDE CONTEST NAMES IN ALL UPPERCASE LETTERS.

(C) FOR COUNTIES THAT USE THE ES&S AND PREMIER VOTING SYSTEMS, ARRANGE THE CONTESTS IN THE ORDER PRESCRIBED BY SECTION 1-5-403(5), C.R.S.
(D) **CAPITALIZE CANDIDATE NAMES** (e.g., **JOHN A. SMITH**).

(E) **PRESENT A Precinct name as a Ten-digit preciNct number.**

(F) **For counties that use the Hart voting systems, use the “Split_name” field split precinct naming purposes.**

(G) **Create a “Provisional” precinct.**

(H) **USE ONLY THE party codes certified by the Secretary of State.**

(I) **Do not include the party name or code in the candidate name field.**

11.11.2 **No later than eight days before the election, a county must send the following information to the Secretary of State, at the address in Rule 11.8:**

(A) A DATA ENTRY COUNTY MUST EMAIL A SAMPLE.

(B) A MANUAL ENTRY COUNTY MUST SEND A LIST OF CONTESTS TITLES, CANDIDATES, AND PARTY AFFILIATION.

11.11.3 **The county must export or produce election results and upload them to the ENR system a minimum of three times on election night:**

(A) **After the close of polls but no later than 7:30 PM.**

(B) **At or around 9:00 PM.**

(C) **At the conclusion of tabulation, the county must indicate that election night reporting is complete in the ENR system.**

11.11.4 **After canvass the county must export or produce election results, and check the appropriate box in the ENR system to indicate that the canvass upload is complete.**

**Rule 12. Recall**

32.2.12.1 **Signature requirements**

32.2.12.1.1 **For petitions to recall school district directors the petition must be signed by the eligible electors of the director’s district equal in number to at least 40% of the ballots cast in the district in the last preceding election at which the director to be recalled was elected as indicated by the pollbook or abstract for the election.** See section 1-12-105, C.R.S.

32.2.12.1.2 **When determining the number of required valid signatures for an elected office for which electors were allowed to vote for more than one candidate in a single race, the signature requirements shall be based on the number of ballots cast for that race as indicated by the pollbook or abstract for the election.**
32.6-12.2 In accordance with section 3 of article XXI of the Colorado constitution and
section 1-12-117(1), C.R.S., for partisan recall elections involving a state officer, in
order to appear on the ballot a successor candidate must file a nomination petition with
the Secretary of State no later than ten calendar days after the Governor sets the election
date. A write-in candidate must file an affidavit of intent to run as a write-in candidate no
later than the fifteenth day before the election.

32.6-12.3 In accordance with section 3 of article XXI of the Colorado constitution and
section 1-12-117(1), C.R.S., for partisan recall elections involving a state officer, in order
to appear on the ballot a successor candidate must file a nomination petition with the
Secretary of State no later than ten calendar days after the Governor sets the election date. A write-in candidate must file an affidavit of intent to run as a write-in candidate no
later than the fifteenth day before the election.

[Current Rule 32.6, adopted on a temporary basis on July 22, 2013, is moved to new Rule 12.3]

Rule 13. Election and HAVA Complaints

13.1 Election Complaint Procedures

13.1.1 Any person who has personally witnessed a violation of Title 1, C.R.S.
may file an election complaint.

13.1.2 An election complaint must include the approved Secretary of State’s
Election Complaint cover sheet.

13.1.3 Processing and Docketing Election Complaints

(A) Within three business days of receiving a complaint, Election Division staff will review the complaint to determine if it satisfies Rule 31.2 and sufficiently alleges a violation.

(i) If the complaint does not meet the criteria, Election Division staff will notify the complainant of the discrepancy.

(ii) If a complaint meets the criteria, Election Division staff will assign a complaint number, notify the complainant, and send a copy of the complaint to the person or entity alleged to have committed a violation.

(B) After notification, the person or entity alleged to have committed the violation will have 15 business days to submit a written response to the Secretary of State’s office.

13.1.4 Amending an Election Complaint

(A) A complainant may amend a complaint within seven days after filing if he or she discovers new facts relating to the existing
COMPLAINT.

(B) An amendment may not contain allegations of a new violation.

13.1.5 Investigation

(A) After the response period outlined in Rule 31.3.2, Election Division staff will investigate the complaint.

(B) If the Secretary of State determines an immediate investigation is required, Election Division staff will begin investigating before the response period has closed. In making the determination, the Secretary will consider whether the issue has the potential to affect an upcoming election.

(C) Depending on the violation alleged, Election Division staff may:

(i) Review documents;

(ii) Visit the county;

(iii) Conduct interviews;

(iv) Test equipment; or

(v) Take other steps necessary.

(D) While an investigation is ongoing, county clerk and recorders and staff must accommodate requests by Election Division staff in the timeframe requested by staff.

13.1.6 Resolution of election complaints

(A) After an investigation and hearing, if applicable, Election Division staff will:

(i) Dismiss the complaint as not supported by credible evidence;

(ii) Refer the complaint to a prosecuting authority under Article 13, C.R.S.; or

(iii) Find a violation and recommend a resolution.

(B) Election Division staff will forward the recommendation for resolution to the Secretary of State, who will adopt, amend, or reject the recommendation.

13.1.7 The Secretary of State’s determination is a final agency action
13.2 HAVA COMPLAINT PROCEDURES

13.2.1 Any person who has been personally aggrieved by or has personally witnessed a violation of Title III of the Help America Vote Act (HAVA) may file a HAVA complaint with the Secretary of State.

13.2.2 A HAVA must include the approved Secretary of State’s HAVA complaint cover sheet.

13.2.3 Processing and docketing HAVA complaints

(A) Within three business days of receiving a complaint, Election Division staff will review the complaint to determine if it satisfies Rule 31.2 and sufficiently alleges a violation.

(I) If the complaint does not include a cover sheet, Election Division staff will notify the complainant of the discrepancy.

(II) If a complaint does not sufficiently allege a violation of Title III of HAVA, Election Division staff will dismiss the complaint without prejudice.

(III) If a complaint meets both criteria, Election Division staff will assign a complaint number, notify the complainant, and send a copy of the complaint to the person or entity alleged to have committed a violation.

(B) After notification, the person or entity alleged to have committed the violation will have 15 business days to submit a written response to the Secretary of State’s office.

13.2.4 Amending a HAVA complaint

(A) A complainant may amend a complaint within seven days after filing if he or she discovers new facts relating to the existing complaint.

(B) An amendment may not contain allegations of a new violation.

13.2.5 Investigation

(A) After the response period outlined in Rule 31.3.2, Election Division staff will investigate the complaint.

(B) If the Secretary of State determines an immediate investigation is required, Election Division staff will begin investigating before the response period has closed. In making the determination, the
Secretary will consider whether the issue has the potential to affect an upcoming election.

(C) Depending on the violation alleged, Election Division staff may:

(i) Review documents;

(ii) Visit the county;

(iii) Conduct interviews;

(iv) Test equipment; or

(v) Take other steps necessary.

(D) While an investigation is ongoing, county clerk and recorders and staff must accommodate requests by Election Division staff in the timeframe requested by staff.

13.2.6 Hearing and Resolution of HAVA Complaints

(A) If the complainant requests, the Secretary of State or his or her designee will hold a hearing.

(B) After the investigation and hearing, if any, Election Division will:

(i) Dismiss the complaint as not supported by credible evidence;

(ii) Refer the complaint to a prosecuting authority under Article 13, C.R.S.;

(iii) Find a violation and recommend a resolution.

(C) Election Division staff will forward the recommendation for resolution to the Secretary of State, who will adopt, amend, or reject the recommendation.

13.2.7 The Secretary of State’s determination is a final agency action.

[Current Rule 31 is repealed and complaint rules are moved to new Rule 13 as shown above.]

Rule 14. Rules Regulating Voter Registration Drives

44.1-14.1 Statement of Intent

44.1-14.1.1 In accordance with section 1-2-701, C.R.S., et seq., the organizer of a Voter Registration Drive (“VRD”) shall must file a Statement of Intent and Training Acknowledgment Form with the Secretary of State to conduct a
voter registration drive on a form prescribed by the Secretary of State. The Statement of Intent shall include the following information:

(a) The name of the group conducting the VRD, and the name and contact information of the individual organizing the VRD;

(b) The name of the agent (who is required to be a Colorado resident) and the contact information for that agent, if different from the person organizing the VRD;

(c) A statement specifying that the VRD intends to operate within the State of Colorado;

(d) A notice that the VRD number expires at the end of the calendar year; and

(e) A signature line requiring the organizer’s signature.

44.1.2 Any amendments to the Statement of Intent shall be filed in writing with the Secretary of State no later than three business days after the change(s) occurs. Amendments may be made by fax, email, mail or in person.

44.1.3 The Secretary of State shall immediately attempt to verify the information provided in the Statement of Intent prior to issuing a number to the VRD organizer. The Secretary of State may deny a number to the voter registration drive organizer if the information provided on the Statement of Intent cannot be verified.

44.1.4 The last day for a VRD to file a Statement of Intent with the Secretary of State shall be IS THE 22ND day before the General Election in a given calendar year.

44.2 Training

44.2.1 In order to be issued a VRD number, the organizer MUST successfully complete the online training and test provided by the Secretary of State, and submit a Statement of Intent along with a Training Acknowledgment form to the Secretary of State.

44.2.2 In addition to training for the organizer, the Secretary of State shall make available information for the organizer to train individual circulators. Organizers MUST provide training to all circulators. Organizers MUST obtain and maintain on file signed attestations from each circulator that he or she will adhere to all the requirements of the Secretary of State election rules and the Colorado Revised Statutes pertaining to elections, and that they are aware of the penalties associated with the mishandling of voter registration application forms.
The organizers shall must furnish the circulator attestations to the secretary of state upon request.

44.2.3 The mandatory training provided by the Secretary of State shall will include, but not be limited to:

(a) The use of the VRD Application;

(b) Information on where to obtain the VRD Application;

(c) Information on how to ensure that a VRD Application is filled out completely; including which fields are optional and which are required; and how to fill out the circulator portion of the Application;

(d) Notice of statutory deadlines relating to Voter Registration Applications and VRDs;

(e) The requirements for when and where delivering the completed Voter Registration Applications must be turned in;

(f) Penalties for violating statutory prohibitions including fraud, intimidation, mishandling Applications, failing to turn in Applications and other penalties relevant to VRDs;

(g) The handling and treatment of confidential information on the Voter Registration Applications; and

(h) Notice that circulators shall not cannot be paid per Voter Registration Application, but if compensated, shall they must be paid by the hour or day.

44.2.4 The training shall be is provided online, but if a VRD organizer prefers, he or she may schedule a time to view the training at the office of the Secretary of State.

44.2.5 After completing the training, the VRD organizer must complete the training test and answer the questions 100% correctly before the Secretary of State will issue a VRD number will be issued.

44.2.6 After completing the training and test, the VRD organizer shall must sign a statement of intent and training acknowledgement form confirming that the training and test have been completed and that he or she was informed of rules, laws and penalties relating to voter registration drives.

44.2.7 A Voter Registration Drive organizer must complete the training and test every calendar year in which he or she intends to conduct a VRD.
44.3.1 Number Assigned

After successful completion of the required training and test, and submission of the required forms STATEMENT OF INTENT AND TRAINING ACKNOWLEDGMENT FORM, the Secretary of State shall will assign a unique number to the VRD. After issuing a unique number to the VRD, the Secretary of State shall will:

(a) Advise the VRD organizer of their unique number;

(b) Notify the county clerks within 24 hours after each VRD number has been issued by the Secretary of State; and

(c) Post the agent and the name of the group conducting the drive on the Secretary of State website.

44.3.2 All assigned VRD numbers are valid through December 31 of the year that the number is assigned.

44.4 Voter Registration Drive Voter Application Forms

44.4.1 The Secretary of State shall will approve a standard Colorado Voter Registration DRIVE Application Form to be used by the VRD that shall include a tear-off receipt.

(a) The VRD may also use the National Mail Voter Registration Form. Because the National Mail Voter Registration Form does not include a tear-off receipt, the applicant and VRD are afforded greater protection when the standard Colorado form is used.

44.4.2 The Secretary of State and county clerks shall make available the official approved Colorado Voter Registration Drive Application Forms to the VRD organizer. A VRD ORGANIZER CAN OBTAIN COLORADO VOTER REGISTRATION DRIVE APPLICATION FORMS FROM COUNTY CLERK AND RECORDERS AND THE SECRETARY OF STATE.

44.4.3 The organizer shall be is responsible for placing the VRD number on the application form and the receipt portion of the standard Colorado form.

44.4.4 The person circulating the Voter Registration Application Forms shall ensure that the tear-off receipt on the standard Colorado Application is completed and given to the applicant. The person circulating the voter application forms shall advise the applicant that the receipt may be needed when he or she votes.

44.4.5 The VRD organizer MUST RECEIVE A VRD NUMBER BEFORE HE OR SHE CAN is not eligible to receive the approved Colorado Voter Registration drive DRIVE Application Forms until the organizer has completed training, signed the
statement of intent, completed and signed the Acknowledgement, and been assigned a number.

44.4.6 14.4.5 Any voter registration drive that provides a voter registration application on its website or a link to such voter registration form must direct the applicant to return the completed form directly to the county clerk and recorder of the applicant’s legal residence. No voter registration drive may provide a voter registration form on its website or a link to such voter registration form which instructs or directs, in any way, the applicant to return the completed form to anyone or any group other than directly to the county clerk and recorder of the applicant’s legal residence or, in the case of overseas electors or UOCAVA electors, the county clerk and recorder or the Secretary of State.

44.5 —Repealed.

44.6 14.5 Voter Registration Drive Complaints and fines

44.6.1 14.5.1 Any person, including the Secretary of State, who believes a VRD organizer or circulator has not complied with the requirements of section 1-2-701 et seq., C.R.S., or this Rule 44 may file a written complaint with the Secretary of State.

44.6.2 14.5.2 A written complaint filed with the Secretary of State shall contain the following information:

a.—(A) The complainant’s name;
b.—(B) The complainant’s full residence address and mailing address (if different from residence);
c.—(C) A description of the alleged violation, which may include a reference to the particular statute or rule;
d.—(D) The name and assigned number of the VRD, if known;
e.—(E) The date and location of the alleged violation, if known; and
f.—(F) Other applicable or relevant information

44.6.3 —Repealed.

44.6.4 14.5.3 The Secretary of State shall review all complaints submitted in writing and conduct such investigations as may be necessary and appropriate. If the Secretary of State determines that a violation has occurred, the Secretary of State shall impose a fine in accordance with section 1-2-703, C.R.S., and notify the VRD organizer of:
44.6.4.1 (A) The date and factual basis of each act with which the VRD organizer is being charged;

44.6.4.2 (B) The particular provision of the statute violated; and

44.6.4.3 (C) The amount of the fine imposed.

44.6.5 14.5.4 Notification of violation shall be sent by certified or registered mail, return receipt requested, to the last known address of the VRD organizer.

44.6.6 14.5.5 The VRD organizer may appeal a fine and shall have thirty (30) days following receipt of notification to submit a written response setting forth the reason(s) that the VRD organizer is appealing the fine. The VRD organizer may request, within the thirty (30) days, a hearing with the secretary of state to dispute the fine.

44.6.7 14.5.6 Within thirty (30) days after receipt of the written response, or hearing procedures, the secretary of state shall issue an order affirming or dismissing the imposed fine.

[Current Rule 44 is amended and moved to new Rule 14. Amendments between the current and new rule language are shown below.]

Rule 15. Rules Concerning Preparation, Filing, and Verification of Statewide Initiative Petitions

15.1 PETITION ENTITY license, registration, and filing, and CIRCULATION procedures.

15.1.1 In accordance with section 1-40-135, C.R.S., any person or issue committee A PETITION ENTITY that intends to compensate PAY petition circulators must obtain a petition entity license, PAY A FEE, and register with the Secretary of State prior to compensating any circulator BEFORE CIRCULATING PETITIONS. THE LICENSE APPLICATION MUST INCLUDE:

15.1.2 To apply for a license the designated agent of a petition entity must pay a fee and submit a signed application including:

a. The PETITION ENTITY’S name, address, telephone number, and email address; of the petition entity;

b. The DESIGNATED AGENT’S name AND; of the designated agent;

e. An affirmation that the entity will not pay any circulator more than 20% of his or her compensation on a per signature or per petition basis; and

c. d. An affirmation that at least one representative of the entity THE DESIGNATED AGENT has read and understands Colorado petition laws as
outlined in article 40 of title 1, C.R.S., and has completed the SECRETARY OF STATE’S circulator training program, provided by the Secretary of State.

15.1.2 BEFORE COMPENSATING A CIRCULATOR, To register with the Secretary of State, the designated agent of a licensed petition entity must register with the SECRETARY OF STATE BY SUBMITTING a signed registration form in accordance with section 1-40-135(5)(a), C.R.S., and provide a list of the PROPOSED INITIATIVES initiative numbers that the petition entity will circulate.

A registration form must be submitted for each new initiative petition that will be circulated prior to compensating any circulator for that petition.

A petition entity license expires if the license is not renewed at least one proposal measure INITIATIVE over any two-year period, THE LICENSE EXPIRES. The Secretary of State will notify a petition entity that its license has expired within 30 days from AFTER the date of expiration.

A petition entity whose license has expired may renew its license WITHOUT A FEE by submitting a NEW license application, in accordance with Rule 15.1.2. No fee is required to submit an application to renew an expired license.

Determinations regarding the denial of an application or revocation of a license will be made, or the resolution of alleged violations involving petition entities shall be addressed, in accordance with the requirements of section 1-40-135, C.R.S.

At the time the petition is filed, the proponents shall file with the Secretary of State a copy of the list of circulators and a copy of the list of notaries required by section 1-40-111(4), C.R.S., as well as the campaign finance disclosure report required by section 1-40-121(1), C.R.S.

Petition representatives.

No petition shall be accepted which lists proponents other than the two identified as petition representatives pursuant to section 1-40-104, C.R.S. A PETITION SECTION MUST LIST THE NAMES OF THE TWO PROPONENTS OR THE NAMES OF THE TWO DESIGNATED REPRESENTATIVES, AS DEFINED IN 1-40-104, C.R.S.

The term “PERSON RESPONSIBLE,” AS USED IN For the purposes of section 1-40-118(2.5)(a), C.R.S., the “person responsible” includes but is not necessarily limited to any MEANS A person or entity who circulates a petition, or causes a petition to be circulated, and who commits, authorizes, or knowingly permits fraud as defined in sections 1-40-111(3)(a) and 1-40-135(2)(c), C.R.S., resulting in the collection of THAT RESULTS IN invalid signatures or petition sections.

Petition circulation.
15.3.1 Proponents may begin circulating a petition for signatures at any time. Petition circulation may begin after the title board's final decision of the title board, including disposition of any rehearing motion for rehearing or the expiration of and after the time for filing a rehearing motion for rehearing, and after the Secretary of State has approved the petition format. of the petition as provided in section 1-40-113(1), C.R.S., whether or not an appeal is filed with the Supreme Court pursuant to section 1-40-107(2). If an appeal is filed with the Supreme Court, the six-month period specified in section 1-40-108(1), C.R.S., shall begin on the date that the first signature is affixed to the petition or on the date that the Supreme Court's decision of the Supreme Court becomes final, whichever date occurs first. Signatures shall be counted only if affixed to the petition during the period provided in this rule. Gathered outside of this period are invalid.

15.3.2 The petition circulator shall must provide his or her a permanent residence address as defined in paragraph (a) of this rule on the circulator affidavit. In addition to providing his or her permanent residence address, if the circulator is not a permanent Colorado resident, of Colorado as described in section 1-2-102(1)(a)(i), C.R.S., and paragraph a of this rule, the circulator shall must also provide the address in Colorado where he or she is temporarily living as of the date the affidavit is signed.

a. For purposes of Article 40 of Title 1, C.R.S., and this rule, a circulator's permanent "residence" or "domicile" means his or her principal or primary home or place of abode in which a circulator's habitation is fixed and to which the circulator, whenever absent, has the present intention of returning after a departure or absence, regardless of the duration of the absence. A permanent "residence" or "domicile" is a permanent building or part of a building and may include a house, condominium, apartment, room in house, or mobile home. Except as provided in paragraph (b) of this rule, no a vacant lot, business address, or post office box may be considered a "false address". (Sections 1-2-102(1)(a)(i) and 1-40-121(1)(b), C.R.S.)

b. For the purposes of petition circulator residence address, a homeless circulator shall must provide the address or location where he or she is living as of the date the affidavit is signed. The circulator must provide a physical location; a post office box may not be provided.

c. For the purposes of sections 1-40-106(4)(b), 1-40-111(3)(a), 1-40-121(2)(a), and 1-40-135(2)(c), C.R.S., a circulator's permanent residence address that does not comply with this Rule 15.3.2 is considered a "false address".

15.4 Only one filing of a petition or an addendum is allowed. Proponents may file a petition or addendum only once, and after a petition or an addendum is filed, the petition or the addendum may not be supplemented with additional
signatures AFTER FILING THE PETITION OR ADDENDUM, EVEN IF THE ADDITIONAL SIGNATURES ARE OFFERED BEFORE THE DEADLINE TO SUBMIT THE ORIGINAL PETITION OR ADDENDUM. If additional signatures are submitted after the original filing, such signatures shall not be counted, even if such signatures are submitted within the time permitted by law for the filing of the original petition or addendum.

17.1-15.5 General procedures concerning verification of petitions. PETITION RECEIPT BY SECRETARY OF STATE.

17.1.1-15.5.1 No petition shall be accepted which, except as specified in Rule 15.2.1, the Secretary of State will not accept a petition that lists proponents other than those authorized by law.

17.1.2-15.5.2 When the petitions are received, each section shall be date-stamped and consecutively numbered with a four-digit number. Upon receipt of a petition, Secretary of State staff will date-stamp and consecutively number petition sections with a four-digit number. The number may be printed by a printer, hand-stamped with a manual stamp, or handwritten.

17.1.3 Each petition shall be either an individual sheet for signatures or multiple sheets that are stapled together.

17.1.4-15.5.3 Staff will inspect each petition section shall be checked for evidence of disassembly. If it appears that the section was disassembled, the Secretary of State will reject all entries signatures in the section shall be rejected.

17.1.5-15.5.4 Staff will consecutively number each line the lines on each petition section shall be consecutively numbered. For purposes of this Rule, “line” means the block of information which consists of that contains the printed last name, first name, middle initial, county, signing date, street address, city, and signature of a petition signer is considered a line.

17.1.6-15.5.5 If the number of entries lines is less than the total number of signatures required to certify the measure to the ballot, the Secretary of State will issue a statement of insufficiency shall be issued.

17.1.7-15.5.6 Staff will count each line with writing shall be counted on each petition section. For purposes of this Rule, an “entry” means a counted line with writing and shall be considered an entry. At the bottom of each page, staff will write the number of entries for each on that page of the section shall be written on the page and, on the face of each petition section, staff will write the total number entries for that section shall be written on the face of the petition section.

a.(A) Staff will not count a line that has with no writing or marks on it or a line with completely-crossed-out writing on it as an entry. shall not be considered an entry.
b. A line that has writing on it but is completely crossed out shall not be considered an entry.

e.(B) STAFF WILL COUNT a line which has WITH INCOMPLETE writing, A PARTIAL CROSS OUT, OR WITH WHAT APPEARS ON ITS FACE TO BE AN INVALID SIGNATURE AS AN ENTRY. on it but is incomplete or on its face contains an invalid signature or which is partially crossed out shall be considered an entry to be included in this count.

17.1.8 15.5.7 Additional signatures submitted after the original filing of an initiative petition or addendum, or candidate petition shall be rejected, even if such signatures are submitted to the designated election official within the time permitted by law for the original filing. THE SECRETARY OF STATE WILL NOT ACCEPT OR COUNT ADDITIONAL SIGNATURES AFTER PROPONENTS FILE THE ORIGINAL PETITION OR ADDENDUM.

17.2 15.6 Checking the circulator’s CIRCULATOR affidavit.

15.6.1 17.2.1 The circulator’s affidavit shall be checked for each entry. If the affidavit is not attached and completed, all entries in the section shall be rejected. IF A PETITION SECTION DOES NOT HAVE A COMPLETED CIRCULATOR AFFIDAVIT, THE SECRETARY OF STATE WILL REJECT THE ENTIRE SECTION.

15.6.2 17.2.2 The notary clause at the end of the affidavit shall be checked for each entry. If any information is missing, or if the date on the notary clause is not the same date as the circulator signed the affidavit, all entries in the section shall be rejected. IF A PETITION SECTION DOES NOT HAVE A COMPLETED NOTARY CLAUSE, OR IF THE DATE OF THE NOTARY CLAUSE DIFFERS FROM THE DATE THE CIRCULATOR SIGNED THE AFFIDAVIT, THE SECRETARY OF STATE WILL REJECT THE ENTIRE SECTION.

17.2.3 15.6.3 The circulator’s affidavit shall be checked to assure it has been completed in accordance with the statutory requirements listed below. If the affidavit was not completed in accordance with the requirements listed below, all entries in the section shall be rejected.

a. For candidate petitions, the circulator’s affidavit shall be completed in accordance with section 1-4-905(1) and (2), C.R.S.

b. For initiative petitions, the circulator’s affidavit shall be completed in accordance with section 1-40-111(2), C.R.S.

15.5 15.7 Petition verification. by Random Sample.

15.5.1 15.7.1 Each petition section shall be verified according to the procedures set forth in Rule 17.1. VERIFICATION BY RANDOM SAMPLE.
15.5.2 Preliminary count and random number generation.

a. After counting the entries have been counted for each petition section, a data entry clerk shall enter the following data into the database: SECRETARY OF STATE STAFF WILL ENTER the petition identification number, the petition section number, the page number and the number of entries on the page INTO THE DATABASE.

b. STAFF WILL THEN CREATE a record shall then be created for each entry which record shall contain the petition identification number, petition section number, page number and the entry number. STAFF WILL TALLY the total number of entries submitted for the petition shall be tallied.

c. If the number of entries is less than the total number of signatures required to certify the measure to the ballot, the SECRETARY OF STATE WILL ISSUE a statement of insufficiency. shall be issued.

d. A series of random numbers shall be generated by the database which is the greater of four thousand (4,000) signatures or five percent (5%) of the total number of entries.

15.5.3 Verification of Selected Entries

a. The random numbers selected shall be matched with the appropriate petition section, page number, and entry number.

b. Each entry generated shall be checked for validity in accordance with Rule 17.4.

c. Each reason for rejection of an entry shall be recorded by separate code and a master record of the rejected entries shall be maintained. A master record shall also be maintained of each entry that is accepted.

15.7.3 Random sample. The database will generate a series of random numbers equal to 4,000 signatures or five percent of the total number of signatures, whichever is greater. Staff will check the validity of the random signatures in accordance with this rule. Staff will maintain a master record of each accepted signature, as well as a record of each rejected signature along with the reason for the rejection.

15.7.4 Checking the circulator’s affidavit. The circulator’s affidavit shall be checked for each entry in accordance with Rule 17.2. Staff will verify that the circulator’s affidavit meets the standards of this Rule 17. If the affidavit is not attached and completed, all entries in the section shall be rejected.
15.5.5 Checking individual signatures. Each individual signature shall be checked in accordance with Rule 17.3.

15.5.6 Computation of total accepted signatures.

a. (A) STAFF WILL KEEP a tally shall be made of the number of accepted signatures and the number of rejected signatures.

b. (B) The Secretary of State shall determine the range of signatures by multiplying the constitutionally required number of signatures by 0.90 to compute ninety percent (90%) of the required signatures and by 1.10 to compute one hundred and ten percent (110%) of the required signatures. This number shall be calculated after the general election at which the Secretary of State was elected.

c. (C) After completing a petition, the number of signatures checked shall then be divided into the number of accepted signatures. This number will be the percentage of accepted signatures which were submitted. STAFF WILL THEN DIVIDE THE NUMBER OF ACCEPTED SIGNATURES BY THE TOTAL NUMBER OF SIGNATURES SUBMITTED TO DETERMINE THE PERCENTAGE OF ACCEPTED SIGNATURES.

d. (D) The percentage calculated in paragraph c of this Rule 15.5.6 shall then be multiplied by the total number of entries which were previously tallied. This number will be the number of presumed valid signatures which were submitted. STAFF WILL THEN MULTIPLY THE PERCENTAGE OF ACCEPTED SIGNATURES BY THE TOTAL NUMBER OF SIGNATURES SUBMITTED TO DETERMINE THE NUMBER OF SIGNATURES PRESUMED TO BE VALID.

e. (E) If the number generated is:

(i) Ninety percent (90%) or less of the constitutionally required number of signatures as calculated in paragraph b of this Rule 15.5.6, then the Secretary of State shall issue a statement of insufficiency. If the number generated is

(ii) One hundred and ten percent (110%) or more of the constitutionally required number of signatures, then the Secretary of State shall issue a statement of sufficiency.

(iii) More than ninety percent but less than one hundred ten percent of the required number of signatures, The Secretary of State’s staff will review every signature to determine sufficiency.

f. If the number generated is more than ninety percent (90%) but less than one hundred and ten percent (110%) of the required number, the Secretary
of State shall order that each signature on the petition be verified to
determine whether the issue or question should be certified to the ballot.

47.3-15.8 Checking verifying individual signatures.

47.3.1-15.8.1 STAFF WILL CHECK each individual entry shall be checked against the
information contained in SCORE. STAFF WILL CHECK each individual entry
shall be checked against the information contained in SCORE. master voter registration files to assure
that the elector was an eligible elector in the political subdivision at the time the
petition was signed.

47.3.2-15.8.2 Each reason for rejection of an entry shall be recorded by separate code
and a master record of the rejected entries shall be maintained. STAFF WILL CREATE AND
maintain a master record of each accepted entry, along
with the reason code for each rejected entry.

47.3.3-15.8.3 If the information on the current voter registration file does not match the
information on the entry, the elector’s voter registration history shall be checked
to determine if the information on the entry matches the voter registration file at
the time the entry was signed. If an entry does not match the signor’s
current information in SCORE, STAFF MUST CHECK THE SIGNOR’S
information in SCORE as of the date the signor signed the petition.

47.3.4-15.8.4 Name of eligible elector. To be accepted, the name on the entry must be in
a form similar to that found on the voter registration record. Signatures that are
common variants of the name found on the voter record shall be counted. If the
signer of the petition is not found on the voter registration file, or if applicable,
the county assessors’ list, the entry shall be rejected. SECRETARY OF STATE
STAFF WILL REJECT THE ENTRY IF:

(A) The name on the entry is not in SCORE;

(B) The middle initial or middle name on the entry does not match the
middle initial or middle name in SCORE;

(C) The address on the entry does not match the address in SCORE;

(D) The address on the entry is a post office box;

(E) The entry is incomplete;

(F) The signer completed the entry before the designated election
official approved the petition format;

(G) The signer was not an eligible elector at the time he or she
completed the entry;

(H) The signer completed the entry after the date on the circulator
AFFIDAVIT;

(I) Evidence exists that some other person assisted the signer in completing the entry but no statement of assistance accompanies the entry;

(j) The name and signature on the entry is illegible and cannot be verified in SCORE;

(k) The entry is a duplicate of a previously accepted entry on the same petition; or

(l) For a candidate petition where an elector may sign only one petition for the same office, the entry is a duplicate of a previously accepted entry on another petition for the same office.

15.8.5 Secretary of State staff will accept the entry if:

(a) The name on an entry matches or is substantially similar to the information in SCORE, or if the signature on an entry is a common variant of the name;

(b) A middle initial or middle name is present on the entry but not in SCORE, or present in SCORE but not on the entry;

(c) A suffix is present on the entry but not in SCORE, or present in SCORE but not on the entry; or

(d) The address on the entry is missing an apartment letter or number or a street direction.

17.4 Final Tally. After all of the sections have been checked, a final tally of all valid signatures shall be prepared and the statement of sufficiency or insufficiency issued.

[Current Rule 19 is amended and moved to Rule 15.9. Amendments between the current and new rule language are shown below.]

19.1 Cure of petitions deemed insufficient. Curing insufficient petitions.

19.2 15.9.1 If the petition proponents submit additional signatures within the permitted time, all signatures submitted in the addendum shall be checked using the process delineated in Rule 16 and Rule 17 Secretary of state staff will verify the additional signatures in accordance with this Rule 15.

19.3 15.9.2 If the number of additional valid signatures, in the addendum when added to the number of valid signatures given in the statement of insufficiency, equals 110% or more of the required signatures, the Secretary of State will issue a statement of
sufficiency. shall be issued.

19.4 15.9.3 If the number of ADDITIONAL valid signatures, in the addendum when added to the number of valid signatures given in the statement of insufficiency, equals more than 90% but less than 110% of the required signatures and if the initial check was by random sample, all of the previously submitted entries shall be checked. STAFF WILL VERIFY ALL PREVIOUSLY SUBMITTED SIGNATURES. STAFF WILL ADD the total number of valid signatures in the original petition shall then be added to the number of ADDITIONAL valid signatures submitted in the addendum.

19.5 15.9.4 If the initial check was of every entry SIGNATURE, then STAFF WILL ADD THE NUMBER OF ADDITIONAL VALID SIGNATURES TO DETERMINE SUFFICIENCY. the total of valid signatures shall be added to the number of valid signatures submitted in the addendum.

19.6 15.9.5 The designated election official shall then issue a new statement of insufficiency or sufficiency which reports the total number of valid signatures submitted.

[Current Rule 20 is amended and moved to new Rule 15.10. Amendments between the current and new rule language are shown below.]

15.10 PETITION PROTESTS.

20.1 15.10.1 A PETITION protest shall—MUST specifically state the reasons for the challenge to CHALLENGING the determination of sufficiency or insufficiency.

20.1.1 (A) A protest that alleges—ALLEGING THE VIOLATION OF A specific statute or rules—STATUTE OR RULE were improperly applied shall clearly state the specific requirements that were improperly applied—MUST CITE THE STATUTE OR RULE AND SPECIFICALLY STATE THE VIOLATION.

20.1.2 (B) A protest that alleges that entries were improperly accepted or rejected shall clearly identify the specific individual entries at issue and the reason the entries were improperly accepted or rejected—ALLEGING THE IMProPER ACCEPTANCE OR REJECTION OF INDIVIDUAL ENTRIES MUST CITE THE ENTRY AND PETITION SECTION NUMBER AND SPECIFICALLY STATE WHY THE ENTRY SHOULD BE ACCEPTED OR REJECTED, AS APPLICABLE.

20.2 The protest shall be deemed insufficient for each entry or class of entries challenged where the individual entry is not listed or the reason for the challenge is not given.

20.3 Where a petition verified by random sample is protested, proponents and opponents may protest the process by which the numbers used in the calculations were generated.

20.4 Individual entries which were not checked by the Secretary of State may not be challenged as sufficient or insufficient.
Current Rule 23 is amended and moved to new Rule 15.11. Amendments between the current and new rule language are shown below.

15.11 REFERENDUM PETITIONS.

23.1-15.11.1 Applicability. This Rule 23 applies to statewide referendum petitions pursuant to article V, section 1 (3) of the Colorado Constitution.

23.2 Relationship to statutory and constitutional provisions.

23.2.1 The purpose of this Rule 23 is to administer and interpret, but not supersede, the provisions of Article V, Section 1, Colorado Constitution, and Article 40 of Title 1, Colorado Revised Statutes which apply to referendum petitions.

23.2.2 Where there is an irreconcilable conflict between this Rule 23 and any such statutory or constitutional provision, then such statutory or constitutional provision prevails.

23.3 Applicability of initiative statutes.

23.3.1-15.11.2 Except where this Rule states otherwise, provides, or where the context otherwise requires, any statutory or constitutional provision that applies specifically to initiative petitions shall also apply to referendum petitions.

23.3.2-15.11.3 The following procedural steps that apply to initiative petitions do not apply to referendum petitions:

(a) Review and comment by legislative staff on the text of proposed initiated constitutional amendments and initiated laws, pursuant to Article V, Section 1 (5), Colorado Constitution, and section 1-40-105, C.R.S.

(b) Title-setting by the title setting review board established in section 1-40-106, C.R.S.

23.4 Approval of referendum petition form.

23.4.1 No referendum petition shall be printed, published, or otherwise circulated unless the form and the master original to be used for printing or reproduction have been approved by the Secretary of State. Section 1-40-113(1), C.R.S.

23.4.2-15.11.4 PROPONENTS MAY SUBMIT a referendum petition may be submitted to the Secretary of State for approval at any time after the GENERAL ASSEMBLY HAS PASSED THE bill. has been presented to the governor for approval or disapproval. The Secretary of State shall not issue final approval of the referendum petition form until the bill has become law pursuant to article IV, section 11 of the Colorado Constitution.
23.4.3-15.11.5 Each referendum petition section shall consist of the following, in the
order listed: Sections 1-40-113(1), and 1-40-102(6), C.R.S.

(a) The warning as specified in Section 1-40-110, C.R.S.

(b) The heading “Referendum Petition,” followed by the demand upon the
Secretary of State in substantially the following form, in which the
underlined material is only for example:

“To: The Honorable ____________, Secretary of State of the State of
Colorado

We, the undersigned electors of the State of Colorado, do hereby
respectfully petition, order, and demand that Sections 1 to 12, inclusive
(being the entire Act), of House Bill No. 02-1010, by Representatives
Abel, Baker, and Cain, and Senators Smith, Thomas, and Jones, entitled
“Concerning registration requirements for motor vehicles, and, in
connection therewith, authorizing two- and five-year registration periods
and authorizing discretionary vehicle identification number inspections,
and making an appropriation”, passed by the Sixty-third General
Assembly of the State of Colorado, at its regular session in the year
2002, shall be submitted to the voters for their adoption or rejection at the
next biennial regular general election, to be held on Tuesday, the 5th day
of November, 2002, and each of the signers of this petition says:

I sign this petition in my own proper person only, and I am a registered
elector of the State of Colorado, my residence address and the date of my
signing this petition are correctly written immediately after my name, and
I do hereby designate the following persons to represent me in all matters
affecting this petition:”

(c) The name and mailing address of two persons who are designated to
represent the signers thereof in all matters, affecting the same.

(d) The ballot title and submission clause, in the form required by this Rule
23.

(e) The text of the Act, or the item(s), section(s), section, or part(s)
part of the Act, on which the referendum is demanded. See sections 1-
40-110; 1-40-102(6).

(f) Succeeding pages that each contain the warning, the ballot title, and
submission clause, and ruled lines numbered consecutively for electors’
signatures.

(g) A final page that contains the circulator’s affidavit required by section
1-40-111(2), C.R.S.
23.4.4 15.11.6 Each referendum petition section shall include only the matters required by Article 40, Title 1, C.R.S., and this Rule 23, and no extraneous material. Section 1-40-113(1), C.R.S.

23.5 Ballot Title and Submission Clause.

23.5.1 15.11.7 The ballot title shall consist of the title of the act on which the referendum is demanded, followed by the bill number, in substantially the following form, in which the underlined material is only for example:

“An Act concerning registration requirements for motor vehicles, and, in connection therewith, authorizing two- and five-year registration periods and authorizing discretionary vehicle identification number inspections, and making an appropriation, being House Bill No. 02-1010.”

23.5.2 15.11.8 When referendum is demanded on less than an entire Act of the General Assembly, the ballot title and submission clause shall consist of the ballot title preceded by words in substantially the following form, in which the underscored material is only for example, and ending in a question mark:

“Shall Section 3 (concerning definition of terms) and Section 4 (eliminating licensing requirements for motor vehicle dealers) of the following Act of the General Assembly be approved?” The material in parentheses shall correctly and fairly summarize the subject or the effect of the portion of the Act referenced.

23.6 15.11.9 Election. If a referendum petition is timely filed with the Secretary of State with a sufficient number of valid signatures, it shall be voted upon at the next general election that occurs at least three months after the referendum petition is filed with the Secretary of State.

[Rules 15, 17, 19, 20, and 23 are amended and relocated to Rule 15.]

Rule 16. MILITARY AND OVERSEAS VOTERS (UOCAVA)

25.1 16.1 General rules concerning voting by military and overseas electors.

25.1.1 16.1.1 For the purposes of this Rule 25, elector means a covered voter as defined in section 1-8.3-102(2), C.R.S.

25.1.2 16.1.2 In accordance with the Help America Vote Act of 2002 and this Rule 25, each county clerk and recorder office shall have a dedicated fax machine for the purpose of fax ballot transmission.

25.1.3 16.1.3 In accordance with section 1-8.3-109, C.R.S., a mail-in-ballot application submitted by an elector shall be effective through the next regularly scheduled General Election, unless the elector specifies otherwise.
25.1.4-16.1.4 Mail-in ballot application—APPLICATION and replacement ballot request

deadlines.

(a) Notwithstanding any other provision of law, an elector may submit an application for registration and ballot request with his or her voted ballot as long as the ballot is timely submitted and received under sections 1-8.3-111 and 1-8.3-113, C.R.S., and Rule 25.1.6.

(b) An application for a mail-in ballot must be received no later than the close of business the Friday immediately preceding the election, except that if the elector who wishes to receive the ballot by mail must submit a request no later than the seventh day before the election, the application must be received no later than the seventh day before the election.

(b) A request for a replacement ballot must be received by 5:00 p.m. MT on election day. A request for replacement ballot includes a request for an electronically transmitted ballot by an elector who has already been issued a ballot by regular mail.

25.1.5-16.1.5 Use of a Federal Write-in Absentee Ballot (FWAB) as an application for registration or ballot request.

(a) In accordance with section 1-8.3-107, C.R.S., Notwithstanding any other provision of law, if an unregistered elector submits a FWAB by the close of registration deadline set forth in sections 1-8.3-111 and 1-8.3-113, C.R.S., and Rule 25.1.6., the FWAB shall be considered a timely application for registration and mail-in ballot request.

(b) In accordance with section 1-8.3-108(4), C.R.S., if a registered elector submits a FWAB no later than the Friday before the election, the FWAB shall be considered a timely application for mail-in ballot.

25.1.6-16.1.6 In accordance with sections 1-8.3-110 and 1-8.3-113, C.R.S., all ballots cast must be voted and mailed or electronically transmitted no later than 7:00 p.m. MT on election day, and received by the county clerk and recorder or the Secretary of State no later than the close of business on the eighth day after election day.

25.1.7-16.1.7 Ballots received by the Secretary of State

(a) If the Secretary of State timely receives a ballot in accordance with this section, the Secretary of State will immediately notify the appropriate county clerk and recorder and forward the ballot by overnight mail, fax, or courier by the most efficient means available no later than the next business day.
(b) To ensure voter secrecy, any county notified that the Secretary of State has received a ballot, shall—MUST retain a minimum of ten voted ballots to be counted with the ballot received by the State.

25.1.8 16.1.8 The county clerk and recorder shall—MUST send a minimum of one correspondence prior to—BEFORE the Primary Election to each elector whose record is marked “Inactive” and whose ballot request has expired. Such shall THE correspondence may be sent by email or mail and, at a minimum, shall MUST notify the electors of:

(a) The status of the elector’s record and ballot request;

(b) The upcoming federal elections;

(c) How to update the elector’s mailing information and request a ballot; and

(d) Any other information the county clerk and recorder deems appropriate.

25.1.9 16.1.9 Reporting. No later than 60 days after a General Election, the county clerk and recorder shall—MUST provide a must report to the Secretary of State in the approved format, which shall summarize in detail the ballots transmitted and returned by military and overseas electors. NO LATER THAN 45 DAYS BEFORE AN ELECTION, THE COUNTY CLERK AND RECORDER MUST REPORT TO THE SECRETARY OF STATE THE NUMBER BALLOTS TRANSMITTED TO MILITARY AND OVERSEAS ELECTORS BY THE 45-DAY DEADLINE.

25.2 16.2 Electronic ballot transmission (receipt and return) of ballots to military and overseas electors.

25.2.2–16.2.1 Electronic Transmission (receipt and return) of ballots to military and overseas electors. (a) In accordance with sections 1-8.3-110 and 1-8.3-113, C.R.S., an elector may request to receive and return his or her ballot by electronic transmission.

(i) Subject to the deadlines in Rule 25.1.4, a request for electronic ballot transmission may be made on the federal postcard, state voter registration, mail-in ballot, online voter registration, or any other application.

(ii) (A) An elector who requests fax transmission shall—MUST provide a fax number, including the international country code and local area, province, or city code (if applicable) where the ballot is to be faxed.

(iii) (B) An elector who requests email transmission shall—MUST provide a complete email address where the ballot is to be transmitted. In accordance with section 1-8.3-115, C.R.S., no election official may disclose the email address to the public.
(b)(c) An elector who chooses to receive his or her unvoted ballot by online ballot delivery may return his or her ballot by fax or email.

(e)(d) To return a voted ballot and self-affirmation by email, the elector must scan and return the documents as an email attachment.

[Current Rule 25.2.1 is moved to Rule 1.]

25.2.4 The ballot packet sent by electronic transmission shall—MUST be in text format on 8 ½” x 11” white paper and shall—MUST include:

(a) An electronic transmission coversheet to protect voter privacy;

(b) The blank ballot;

(c) The electronic transmission ballot instructions; and

(d) The self-affirmation required by section 1-8.3-114, C.R.S.

25.2.5 The electronic transmission ballot instructions shall—MUST include:

(a) The county clerk and recorder’s contact information including mailing address, email address, phone, and fax number;

(b) A notice that the ballot may not be duplicated for any other elector;

(c) Instructions for completing and returning the ballot;

(d) A notice regarding the ballot return deadline;

(e) Information regarding how the elector may verify that his or her ballot has been received by the county clerk and recorder; and

(f) Any other information deemed necessary by the Secretary of State or the designated election official.

25.2.6 The self-affirmation shall—MUST include the standard oath required by the Uniformed and Overseas Citizen Voting Act (42 U.S.C sec. 1973ff(b)(7) and 1(a)(5)), the elector’s name, date of birth, signature, and the following statement: I also understand that by returning my voted ballot by electronic transmission, I am voluntarily waiving my right to a secret ballot. (Section 1-8.3-114, C.R.S.)

25.2.7 Any ballot transmitted to an elector by electronic transmission shall—MUST contain a unique identification number for tracking and auditing purposes.

25.2.8 If the county clerk and recorder transmits a ballot packet to an elector by fax and the transmission is unsuccessful, the county clerk and recorder shall attempt to fax the ballot at least two more times.
25.2.9 – 16.2.7 The county clerk and recorder shall MUST maintain a log of each ballot sent by electronic transmission, which the county CLERK AND RECORDER shall MUST maintain THE LOG as an election record along with any other email or fax records. The log shall MUST include:

(a) The name of the elector;

(b) The fax number or email address to which the ballot packet was transmitted (as applicable);

(c) The unique identification number of the ballot;

(d) The date the ballot packet was transmitted; and

(e) The initials of the employee transmitting the ballot.

25.2.10 – 16.2.8 Upon receipt of a voted ballot sent by electronic transmission, the county clerk and recorder shall MUST verify the elector’s signature in accordance with Rule 29, and upon verification the ballot shall be duplicated for counting. AFTER THE AFFIDAVIT HAS BEEN VERIFIED, A BIPARTISAN TEAM OF JUDGES MUST DUPLICATE THE BALLOT. DUPLICATING JUDGES MUST NOT REVEAL HOW THE ELECTOR HAS CAST HIS OR HER BALLOT.

13.20 – 16.2.9 A military or overseas elector whose registration record is inactive or whose ballot request has lapsed may download an application and ballot using the electronic ballot delivery system.

13.20.1 (A) The elector must submit the ballot and application in accordance with the deadlines in section 1-8.3-111 and 1-8.3.113, C.R.S., for the ballot to be counted.

13.20.2 (B) Every county must use the approved electronic delivery system to implement this rule, except that a county may obtain a waiver. The Secretary will consider the following factors in approving or denying a request for waiver:

(a) (I) Number of military or overseas electors registered to vote in the county;

(b) (II) Historical data regarding the number of military and overseas electors who have registered and voted in the county; and

(c) (III) Staff or other resource limitations.
[Current Rule 25 is amended and moved to new Rule 16. Current Rule 13.20 is amended and moved to new Rule 16.2.9. Amendments between the current and new rule language are shown above.]

Rule 17. PROVISIONAL VOTING

17.1 PROVISIONAL VOTING IN THE VOTER SERVICE AND POLLING CENTER

17.1.1 The county clerk and recorder must use the approved provisional ballot form.

17.1.2 If a voter service and polling center loses connectivity to SCORE, the judges must issue provisional ballots until the county restores connectivity.

[Current Rule 26.3.3 is amended and moved to new Rule 17.1.3. Amendments between the current and new rule language are shown above.]

26.4.17.2 Verification of Provisional Ballots

17.2.1 The county clerk and recorder must process and tabulate all regular ballots before processing provisional ballots.

26.12.17.2.2 The county clerk and recorder must process all pollbooks or signature cards in the statewide voter registration database system before processing provisional ballots.

[Current Rule 26.12 is moved to new Rules 17.2.]

26.4.2.17.2.3 Verification of an elector’s eligibility to have his or her provisional ballot counted shall be limited to the following sources:

(a) Sources provided by the Secretary of State or law enforcement agencies regarding felons who are serving a sentence of detention or confinement or on parole;

(b) The State of Colorado Statewide Voter Registration Database;

(c) The DMV Motor Voter database (Note: Possession of a driver’s license is not conclusive proof of voter registration; elector must have registered to vote through the DMV); and

(d) The information provided on the provisional ballot envelope, including the affidavit.
26.4.3-17.2.4 When verifying provisional ballots, the designated election official shall
must check the State of Colorado Statewide voter registration database to
determine whether the elector has already voted in the election.

[Current Rules 26.4.2 and 26.4.3 are amended and moved to new Rules 17.2.3 and
17.2.4. Amendments between the current and new rule language are shown above.]

26.4.5-17.2.5 If during verification it appears that the elector’s record was cancelled or
consolidated as a duplicate in error, the ballot shall must be counted so long as
the elector has not cast a ballot in the election, the affidavit is complete, and the
elector is otherwise eligible. THE COUNTY CLERK AND RECORDER MUST REINSTATE
OR UNCONSOLIDATE THE ELECTOR’S RECORD AND UPDATE THE ELECTOR’S RECORD
BEFORE MARKING THE ELECTOR’S PROVISIONAL BALLOT AS ACCEPTED OR REJECTED
IN THE STATEWIDE VOTER REGISTRATION SYSTEM AND BEFORE LINKING IT TO THE
ELECTOR’S RECORD. IT shall be reinstated or unconsolidated.

26.4.6-17.2.6 When the designated election official has received both a mail-in
MAIL ballot and a provisional ballot from an elector, but there is a discrepancy
between the signature on the returned mail-in MAIL ballot envelope and the
elector’s signature stored in the statewide voter registration system, the
discrepancy must be resolved. Before the provisional ballot may be counted
VERIFIED, the elector must affirm that the signature on the mail-in MAIL ballot
envelope is not his or her signature. Section 1-8.5-105(4) and (5), C.R.S.

[Current Rules 26.4.5 and 26.4.6 are amended and moved to new Rules 17.2.5 and
17.2.6. Amendments between the current and new rule language are shown above.]

26.4.9-17.2.7 If an an elector whose voter registration record is tagged ID required
casts a provisional ballot without providing valid identification, the ballot shall
must be verified and counted as follows:

(a) The COUNTY CLERK AND RECORDER MUST SEND THE ELECTOR shall be sent a
letter within three days after the ballot is cast, and no later than three days
after election day, explaining that he/she has not provided the required
identification. Nothing in this rule shall shall be construed to prohibit the
designated election official PROHIBITS THE COUNTY CLERK from calling the
elector; however, a phone call does not substitute for notification to
the elector in writing.

(b) If the elector provides a copy of valid identification within eight days after
election day, the ballot shall must be counted so long as the elector has
not cast another ballot in the election, the affidavit is complete, and the
elector is otherwise eligible.

[Current Rule 26.4.9 is amended and moved to new Rule 17.2.7. Amendments between
the current and new rule language are shown above.]
26.5.1-17.2.8 If the information contained in the provisional ballot envelope and affidavit provides adequate criteria so that the designated election official is able to confirm under election Rule 26 that the elector is eligible to cast a ballot, the provisional ballot shall MUST count.

[Current Rule 26.5.1 is amended and moved to new Rule 17.2.8. Amendments between the current and new rule language are shown above.]

26.5.3-17.2.9 Acceptance Codes (Any provisional ballot given an acceptance code shall have all--THE COUNTY CLERK AND RECORDER MUST COUNT ALL races counted unless otherwise indicated.)

AOK Reviewed and confirmed voter’s eligibility.

ALC ELECTOR VOTED A PROVISIONAL BALLOT BECAUSE THE VOTER SERVICE AND POLLING CENTER LOST CONNECTIVITY. ELECTOR’S ELIGIBILITY IS CONFIRMED.

26.5.4-17.2.10 Rejection Codes (Any--THE COUNTY CLERK AND RECORDER MUST NOT COUNT A ballot given a rejection code shall not be counted):

RNS (Rejection not signed) Provisional Ballot Affidavit not signed.

RIN (Rejection incomplete information provided) Required information is incomplete and the designated election official is unable to confirm voter’s eligibility.

REE (Rejection envelope empty) Provisional ballot envelope is empty.

RAB (Rejection voter voted mail-in ballot) Designated election official has confirmed that voter voted a mail-in ballot.

RED (Rejection based upon ballot cast on election day IN PERSON) Voter voted in a polling place. VOTER SERVICE CENTER OR POLLING CENTER

RIP (Rejection based on incorrect party) Incorrect Party in Primary Election.

RFE (Rejection felon not eligible to vote) Individual was convicted of a felony and is either serving a sentence of confinement or detention or is on parole.

RWC (Rejection elector not registered in county or A RESIDENT OF THE State of Colorado) Non-county or non-state VOTER IS NOT A STATE resident; therefore voter not eligible to vote in the county where the provisional ballot was voted.

RID (Rejection first time voter has not supplied identification upon registration or thereafter prior to and during time voter voted) First Time Voter who
registered by mail or through a voter registration drive, is tagged as ID deficient, and did not provide ID at the time of voting.

[Current Rules 26.5.3 and 26.5.4 are amended and moved to new Rules 17.2.9 and 17.2.10. Amendments between the current and new rule language are shown above.]

26.6-17.3 The provisional ballot log required by section 1-8.5-110(4), C.R.S., may be prepared by the designated election official in handwritten or computer-generated form.

26.7-17.4 Recount procedures for provisional ballots shall be the same as the recount procedures for other ballots as directed by the Secretary of State.

[Current Rules 26.6 and 26.7 are amended and moved to new Rules 26.3 and 26.4. Amendments between the current and new rule language are shown above.]

17.5 Processing provisional ballot affidavits in the statewide voter registration database. Before closing an election, the county clerk and recorder must:

17.5.1 Enter all provisional ballot affidavits into the provisional module of the statewide voter registration database.

17.5.2 Process all voter registration updates.

17.5.3 Link all provisional ballot affidavits to the appropriate elector’s record.

[Current Rule 26.11 is amended and moved to new Rule 17.5. Amendments between the current and new rule language are shown above.]

17.6 Public access to provisional ballot information

17.6.1 The list of voters who cast a provisional ballot and the accept/reject code for the ballot is available for public inspection.

17.6.2 In accordance with section 24-72-204(8), C.R.S., the county clerk and recorder must not release an original or copy of the elector’s:

(A) Month and day of date of birth;

(B) Driver’s license or Department of Revenue identification number;

(C) Social security number; or

(D) Signature.

17.6.3 If a voter has requested confidentiality under section 24-72-204(3.5), C.R.S., the county clerk and recorder must not release the elector’s address or telephone number.
17.6.4  IF A VOTER HAS REQUESTED CONFIDENTIALITY UNDER SECTION 24-30-2101, C.R.S., THE COUNTY CLERK AND RECORDER MUST NOT RELEASE THE PROVISIONAL BALLOT AFFIDAVIT.

26.13-17.7  Voter Access to Provisional Ballot Information

26.13-1.17.7.1 The Secretary of State will provide a provisional ballot lookup on the Secretary’s website.

26.13.2.17.7.2 The county clerk and recorder must number the provisional ballot envelope or affidavit stock using the standard numbering convention approved by the Secretary of State.

26.13.3.17.7.3 An elector may access the system during the 45 days following the election.

[Section 1-8.5-111, C.R.S.]

[Current Rule 26.13 is amended and moved to new Rule 17.7. Amendments between the current and new rule language are shown above.]

[Current Rule 26 is amended and moved to new Rule 17. Amendments between the current and new rule language are shown below.]

Rule 18. Uniform Ballot Counting Standards

27.2-18.1 Multiple Page Ballots. In any election where a multiple page printed ballot is used, a voter must vote and return all pages of the ballot at the same time. Any voter who has returned at least one page of a multiple page printed ballot will be considered to have voted and the COUNTY CLERK AND RECORDER MUST COUNT THE VOTES on the submitted PAGES page(s) shall be counted. Any THE COUNTY CLERK MUST NOT COUNT VOTES ON additional page(s) returned at a later time shall not be counted. but shall be appropriately marked, set aside, and preserved.

27.2-18.2 Uniform Counting Standards for hand-counted Paper Ballots

27.3-18.2.1 Pursuant to IN ACCORDANCE WITH section 1-7-309, C.R.S., AND RULE 27.7, judges counting ballots on election day shall MUST take into consideration the intent of the voter in accordance with Rule 27.7.

27.3.2-18.2.2 If a RACE OR BALLOT MEASURE IS OVERVOTED ballot contains markings for more than the maximum votes allowed in a candidate race or for a ballot measure, THE JUDGES MUST no vote shall count NO VOTE for that race or ballot measure.

27.3.3-18.2.3 If a candidate race or ballot measure contains no markings by the voter, no tally will be made for that race or ballot measure. BUT all other candidate
races or ballot measures properly marked by the voter on the ballot shall MUST be counted.

27.3.4 18.2.4 A ballot which has no markings for any candidate races or ballot measures shall MUST be tallied as a blank ballot, but the voter shall MUST be given credit for voting.

27.4 27.3 Uniform Counting Standards for Optical Scan Ballots

27.4.1 18.3.1 Precinct Optical Scan Procedures at a Voter Service and Polling Center

(a) Voters whose ballots are rejected or sorted by the precinct counter as a blank or overvoted ballot shall MUST be given the opportunity to correct their ballot.

(b) Ballots sorted to a write-in bin shall MUST be tallied at the conclusion of the voting and delivered to the central counting center in a secure container.

27.4.2 18.3.2 Central Count Optical Scan Procedures

(a) Judges should complete a visual inspection of every ballot should be completed for the limited purpose of separating damaged ballots into a unique batch.

(b) Judges must resolve, and where applicable, duplicate, every damaged ballot and all ballots sorted by the optical scan machine shall be resolved, and where applicable duplicated, in accordance with this rule.

(c) A resolution board, consisting of a team(s) of one (1) Republican and one Democrat for partisan elections or two (2) qualified election judges for nonpartisan elections, shall MUST resolve all ballots sorted by the central count optical scan equipment.

(1) The board shall MUST be observed by two (2) witnesses, who in any partisan election shall be representatives of each major political party, who may not handle or process ballots.

(2) All persons engaged in the counting and processing of ballots shall MUST be deputized or take an oath to faithfully perform their duties.

(3) The resolution board shall MUST maintain a log for each step of verification, duplication, and counting.

(d) Sequence of Resolution Procedures
1. The resolution board must run a zero tape, or similar report, indicating no votes cast or counted before the counting begins.

2. Official ballots shall be processed through the board must review all ballots with overvotes, blank ballots, and write-in ballots sorted by the optical scanner, with sorted overvotes, blank ballots, and write-in ballots viewed and resolved by the resolution board. Ballots sorted by the optical scan equipment shall be subject to review by the resolution board. If there are no legally qualified write-in candidates, the write-in sort option shall not be utilized.

3. A voter’s intent shall be reviewed for every ballot that requires resolution.

4. All ballots which are sorted by the optical scanner and resolved by the resolution board by duplication are to be indicated as such.

5. The resolution board shall maintain an official audit log for all ballots resolved setting forth the precinct number, duplicate ballot number (where applicable), reason (with specificity) that the ballot was resolved, date of resolution, and the initials of the members of the duplication board responsible for resolving the ballot.

6. The precinct judge’s ballot reconciliation form is compared to the number of scanned ballots for the precinct.

7. After the final precinct has been tallied, the total write-in votes shall be indicated on the final summary along with the seal numbers for each sealed box of scanned ballots.

(e) Resolution of damaged ballots

1. Damaged ballots damaged or defective ballots shall be duplicated utilizing the ballot duplication procedures as provided in Rule 27.6.18.5.

2. Blank ballots shall be examined by the resolution board to determine if the ballot is a true blank ballot or one that has been marked with a non-detectable mark. Resolution board members must make a duplicate copy of the ballot which has been marked with a non-detectable mark utilizing the ballot duplication procedures as set forth in Rule 27.6.18.5. If a ballot is truly blank, the board must send it.
sent back for the resolution pass through the scanner, and the ballot
MUST be tabulated with no races or ballot measures voted.

(3) The resolution board MUST inspect and resolve overvoted
overvoted ballots shall be inspected by the resolution board and
resolved in accordance with Rule 27.7-18.6.

(4) Write-in votes sorted by the optical scan equipment on election day
shall—MUST be delivered to the assigned write-in board for hand
counting.

(i) During the initial ballot count, in order to be counted, the
oval must be darkened or the arrow connected according to
the appropriate voting instructions. Only votes for legally
qualified write-in candidates shall—MAY be counted.

(ii) If, following the initial count, the number of undervotes in
that race could change the outcome or force the election into
a mandatory recount if attributed to a legally qualified write-
in candidate, votes for that candidate shall—MUST be counted
whether or not the target area designating the selection of a
write-in candidate has been marked, provided that the
number of candidates chosen does not exceed the number
permitted in that office.

(5) The resolution board shall—MUST duplicate ballots by clearly
labeling the new duplicate ballot as a “DUPLICATE” and assign a
serial number which shall be recorded on both the original and
duplicate ballot. For example, the first ballot in Precinct # 1 to be
duplicated could be labeled as #1/001 with the duplicate labeled
D#1/001. Original ballots shall—MUST be separated from the
duplicate ballots and placed in a sealable container clearly marked
“ORIGINAL BALLOTS.” The duplicate ballots shall—MUST be
counted in lieu of the original ballots.

(6) The resolution board shall—MUST maintain an official audit log
setting forth the precinct number, duplicate ballot number, reason
(with specificity) that the ballot was duplicated, date of
duplication, and the initials of the members of the duplication
board responsible for duplicating the ballot.

(f) Recount Procedures for Optical Scan

(1) Optical scan equipment must be set to consistent sensitivity
standards for each system type, must be tested prior to the recount,
and shall be programmed to sort undervotes for the individual
race(s) or ballot measure(s) being recounted.
The county will conduct a recount of a race with a write-in candidate as outlined in Rule 27.7.4.18.6.4.

Uniform Counting Standards for DREs. A vote that is properly recorded, as specified by the voting instructions, on the voting device for an office or ballot measure shall MUST be counted.

Duplication of Ballots.

(a) Using the damaged ballot as the guide, THE DUPLICATING TEAM MUST MARK a blank ballot shall be marked by a duplicating team, so that the votes recorded are identical to those indicated on the damaged ballot, and shall THE DUPLICATION MUST be proofed to ensure it is marked properly and accurately.

(b) Every duplicated ballot shall MUST be subject to the process for determining voter intent outlined in Rule 27.7-27.6.

(c) A unique number shall MUST be assigned to both the original and duplicated ballot. This will reference the two ballots together and provide an audit trail. (Example: the ballots may be marked XX-NNN, where XX is the precinct number and NNN are consecutive numbers starting with the number one.)

(d) The duplicated ballots shall MUST be counted in the same manner as all other ballots to be counted.

(e) The damaged or unreadable original ballot shall MUST be marked “DUPLICATED” to indicate that the ballot has been duplicated and the duplication is completed. All duplicated original ballots for a precinct along with any applicable printed material shall MUST be placed in a sealable container and clearly marked “ORIGINAL BALLOTS.”

Determination of Voter Intent

If a voter uses a consistent alternate ballot marking method that deviates from the method specified by the voting instructions (such as circling or placing a check mark behind a candidate’s name or ballot response) and does not place an “X”, check or other appropriate mark in the target area(s) AREA, the voter will be considered to have voted for the appropriate candidates and or ballot responses and the ballot shall MUST be duplicated. except that, BUT if a voter marks any of his/her HIS OR HER choices by placing an “X”, check or other appropriate mark in any target area on the voter’s ballot, only those choices where the target area has been IS marked shall MAY be counted.

A ballot that has a mark correctly in the target area that partially extends into another target area shall MUST be counted as a vote for the candidate or ballot response so marked.
27.7.3-18.6.3 When resolving an overvoted race, marks indicating the voter’s intent shall include, but not be limited to, circling the candidate’s name and strike-outs or corrections of choices.

27.7.4-18.6.4 Write-in votes

27.7.4.1 (A) If a voter designates a vote for a named candidate on the ballot and writes in the name of the same candidate in the write-in area, the vote shall MUST be counted.

27.7.4.2 (B) If a voter designates a named candidate on the ballot and writes in the name of a different candidate in the write-in area, it shall MUST be considered an overvote for that office if the number of chosen candidates exceeds the number permitted to be voted for in that office and no vote shall MAY be counted.

27.7.4.3 (C) During any recount of votes, if the number of undervotes in that race could change the outcome if attributed to a legally qualified write-in candidate, votes for that candidate shall MUST be counted whether or not the target area designating the selection of a write-in candidate has been marked, provided that the number of candidates chosen does not exceed the number permitted in that office.
Rule 32. RESERVED

Rule 33. RESERVED

Rule 34. RESERVED

Rule 35. RESERVED

Rule 36. RESERVED

Rule 37. RESERVED

Rule 38. RESERVED

Rule 39. RESERVED

Rule 40. Rules Concerning Certification and Education of Designated Election Officials

40.1 Purpose and Definitions.

40.1.1 The Secretary of State recognizes that the oversight of elections is a profession that requires thorough knowledge of complex state and federal election law and election procedures. Considering the complexity of state and federal law, voting equipment, and election procedures, extensive training is necessary. The certification program standardizes election procedures and education. The program also promotes Colorado voters’ confidence in their election officials and the election process.

40.1.2 “Local election official” means a county clerk and recorder. (Section 1-1-301(1), C.R.S.)

40.1.3 “Persons required to complete certification” means:

(a) The county clerk and recorder; and

(b) Employees in the clerk and recorder’s office who are directly responsible for overseeing election activities, including but not limited to: voter registration, candidate qualifications and ballot certification, poll worker training, ballot design and setup, ballot counting, and canvassing.

(Section 1-1-302, C.R.S.)

40.2 Advisory Board.

40.2.1 The advisory board must meet at least twice each calendar year to approve the curriculum and make necessary changes. The advisory board must also review evaluations and recommend changes to the certification program.

40.2.2 The advisory board must review individual applications for certification and
must approve applications that are accurate and complete. The advisory board may take into account special circumstances in reviewing and approving applications.

40.2.3 The Secretary of State will appoint the following as board members:
(a) Four county clerks or designated staff members;
(b) Two Secretary of State Office representatives; and
(c) Any individual(s) whom the Secretary of State believes could make a valuable contribution to the Board.

40.2.4 Board members serve at least a two-year term.

40.2.5 The Secretary of State may terminate board members without cause. Failure to attend meetings or meaningfully contribute may result in termination.

40.3 Curriculum.

40.3.1 The Secretary of State will develop the core and elective curriculum offered for certification and continuing elections education. The Secretary will post curriculum information on the Secretary of State’s website.

40.3.2 The Secretary of State will develop and administer all training outlined in this Rule 40.

40.3.3 To obtain Colorado certification, a person must complete the following minimum curriculum prescribed by the Secretary of State:
(a) Seven basic core courses;
(b) One core course relevant to primary job duty; and
(c) Six electives.

40.3.4 To maintain Colorado certification, a person must complete at least five Continuing Elections Education courses by July 31 of every even year.

40.4 Training Format.

40.4.1 Web-based training may be conducted live or by reviewing material previously presented by the Secretary of State. In either case, participants must achieve a satisfactory score on assessments before receiving credit for the course.

40.4.2 The Secretary of State will provide classroom training. For certification, a person must complete at least one course in-class.

40.5 Credit.
40.5.1 Individuals applying for certification must successfully complete the curriculum prescribed by the Secretary of State. If an applicant submits duplicate coursework, the advisory board may reject the application for certification.

40.5.2 Training assessment.

(a) To receive certification credit for any course presented by the Secretary of State under this rule, a participant must successfully complete a training assessment with a minimum score of 85%.

(b) A participant who fails to achieve a score of at least 85% may retake the assessment.

(c) The Secretary of State may administer either paper or electronic assessments.

40.5.3 Credit for Teaching Classes. A person who teaches or substantially assists with preparation of a class offered for certification is excused from the assessment requirement outlined in Rule 40.5.2 and will receive credit for the course.

40.5.4 No election official may receive credit toward his or her Colorado certification for training offered by other agencies or organizations.

40.6 Application Review, Certification, and Maintenance of Records.

40.6.1 Once a person completes the required coursework, he or she must promptly submit an application for certification or continuing certification to the Secretary of State’s office on the form approved by the Secretary of State.

40.6.2 The Secretary of State must review the application with reference to the Secretary of State records. If the application is complete and accurate, the Secretary of State must forward it to the advisory board for its review and approval. Upon approval by the advisory board, the Secretary of State must issue a certificate that the person is a Certified Colorado Election Official.

40.6.3 The Secretary of State must track attendance at all classes and keep records of attendance, continuing elections education, and records of those persons who are certified and persons who are in the certification process.

40.9 Decertification. A person who fails to satisfy continuing education requirements will lose certification.

Rule 41. RESERVED

Rule 42. RESERVED

Rule 43. County Security Procedures
43.1 Definitions.

43.1.1 “Chain-of-custody log” 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 “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 the voter can activate; 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.

43.1.3 “Elector data” means voting information, including but not limited to, voter registration, voting history, and voting tabulations.

43.1.4 “Electronic pollbook” is a list of eligible electors in electronic format who are permitted to vote at a polling location in an election conducted under the Election Code, which shall be processed by a computer at a Vote Center to be immediately accessible to all other computers at all Vote Centers in the county.

43.1.5 “Employee” means all full-time, part-time, permanent, and contract employees of the county who have had a Colorado Bureau of Investigation (CBI) Internet criminal history check (ICHIC) 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.

43.1.6 “Removable card or cartridge” means any—a programming card or cartridge, except a voter activation card, that stores firmware, software, or data.

43.1.7 “Seal” means a serial-numbered tamper-evident device that indicates a seal is broken or removed, IF BROKEN OR MISSING, INDICATES THAT A DEVICE IS NOT SECURE.

43.1.8 “Teleprocessing lines” means secure, dedicated communication transmission facilities used for the purpose of transferring elector data between Vote Centers and a centralized computerized pollbook maintained by the county clerk and recorder, to ensure the security and integrity of voting information so that no deviation can go undetected.
43.1.6 “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 the disk(s), which is then used to establish and/or re-establish the chain of custody of any component of a voting system that contains newly installed firmware or software. The trusted build is the origin of the chain of evidence for any software and firmware component of the voting system.

43.1.7 “Video security surveillance recording” means video monitoring by a device that continuously records a designated location or a system using motion detection that records one frame, or more, per minute until detection of motion triggers continuous recording.

43.2 Annual security plan. In accordance with section 1-5-616(5), C.R.S., AND USING THE FORM PRESCRIBED BY THE SECRETARY OF STATE, each county must annually submit a security plan to the Secretary of State annually and no later than 60 days PRIOR TO the first election in which the COUNTY WILL IMPLEMENT THE security plan procedures are used. The plan must, at a minimum, include the following:

43.2.1 General requirements CONCERNING CHAIN-OF-CUSTODY.

(a) 43.3.1 The county clerk and recorder shall MUST maintain on file all documentation of seals, chain of custody, and other documents related to the transfer of equipment between parties. These documents are subject to inspection by the Secretary of State.

(b) 43.3.2 The county must maintain and document the chain of custody for each voting device throughout the county’s ownership or leasing of the device.

(c) 43.3.3 Only deputized clerks, election judges, or canvass board members sworn under oath are allowed to handle ballots, which include VVPAT records.

(d) 43.3.4 The county may install additional or modified software developed by the vendor 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, provided that the software is included in the certified list of services and executables for the certified voting systems.

(e) 43.3.5 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.

43.3.6 The county shall MUST submit with the security plan sample copies of all referenced forms, schedules, logs, and checklists WITH THE SECURITY PLAN.

[Current Rule 43.3 is moved to Rule 43.3.6]
43.2.2-43.4 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, and indicate by signing and dating the log, that the seal serial numbers match the logged serial numbers. If a seal is inaccessible and cannot be removed, then it is not necessary to verify that seal serial number.

(a) 43.4.1 DREs AND BALLOT MARKING DEVICES. The county must seal DRE voting devices as follows:

(1)(A) The county must place a seal over any removable card or cartridge that is inserted into the unit, or over the slot or door covering the card or cartridge.

(2)(B) The county must place a seal over any removable card slot or cartridge slot when no card or cartridge is inserted into the unit.

(3)(C) If the county cannot verify the firmware or software hash value (MD5 or SHA-1), the county must seal the DRE case. To detect unauthorized access, the county must use seals at either the seams of the case or at key entry points such as screw access points.

(4)(D) If the voting device contains one or more slots for a flash memory card, the county shall affix a seal over each flash card slot, door, or access panel.

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

(6)(F) Two employees or election judges must verify, and indicate by signing and dating the chain-of-custody log, that all seal serial numbers match the logged serial numbers.

(b) 43.4.2 VVPATs. Prior to attaching a VVPAT to a specific voting device, the judges shall seal the unit after verifying that no votes were cast. At least two election judges must verify that seals are intact prior to the start of voting, and at the close of voting. VVPAT records shall either remain in the VVPAT canister, or be sealed and secured in a suitable device for protecting privacy or as described in Rule 44.32.10.

(c) 43.4.3 Remote or central count optical scanners. Optical scanners used in a remote or central tabulating location shall meet the following seal requirements:

(1)(A) The county must place a seal over each card or cartridge inserted into the unit, or over any door or slot containing the card or cartridge.

(2)(B) The county must place a seal over each empty card or cartridge slot or door covering the area where the card or cartridge is inserted.
(3)(c) Prior to the start of voting and after the close of voting, two employees or
election judges must visually confirm that all seals are intact and that the
seal serial numbers match those logged in the chain-of-custody log.

4 43.4.4 Memory Cards/Cartridges - CARDS OR CARTRIDGES.

(1)(A) The county must assign and securely affix a permanent serial number to
each removable card or cartridge. The county may use the manufacturer
assigned serial number for this purpose.

(2)(B) The county must handle removable memory cards and cartridges in a
secure manner at all times. The county must transfer and store any
removable card and/or cartridge that is not sealed in a voting machine in a
secure container with at least one seal. Upon delivery and receipt, election
judges or county personnel must verify, and indicate by signing and dating
the chain-of-custody log, that all seal serial numbers match those listed in
the log.

(3)(C) 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.

43.2.3-43.5 Individuals with access to keys, door codes, and vault combinations.

(a) 43.5.1 For employees with access to areas addressed in Rule 43.2.3(e)-43.5.3, the
county must state the employees’ titles - EACH EMPLOYEE’S TITLE and the dates of
CBI background checks - THE ICHC. [Section 24-72-305.6, C.R.S.]

(b) 43.5.2 The county must change all keypad door codes or locks, vault
combinations, computer and server passwords, encryption key codes, and
administrator passwords at least once per calendar year prior to the first election
of the year.

(c) 43.5.3 Employee access.

(1)—The county may grant employees access to the codes, combinations,
passwords, and encryption keys described in this Rule 43.2.3 43.5 in
accordance with the following limitations:

(A)—Access to the code, combination, password, or encryption key for the
storage area for voting equipment and the mail in ballot counting areas is
restricted to employees as defined in Rule 43.1.3.

(B)(A) Access to the code, combination, password, or encryption key for the
mail in VOTING EQUIPMENT AND ballot storage area AREAS and counting
room or tabulation workstations is restricted to ten employees as defined in Rule 43.1.3 who have passed a Colorado Bureau of Investigation (CBI) Internet Criminal History Check (ICHC).

(C)(B) Except for emergency personnel, no other individuals shall MAY be present in these locations unless supervised by one or more employees as defined in Rule 43.1.3.

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

(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.

[Current Rule 43.2.3 (c)(1)(C)(ii) is amended and relocated to New Rule 43.8.]

(2)(C) In extreme circumstance, the county may request and the Secretary of State may grant exemption from the requirements outlined in Rule 43.2.3(e) 43.5.3.

(d) 43.5.4 Computer room. Access to where election management software is used is limited to authorized employees and election judges only. Messengers or runners delivering ballots between the preparation room and computer room shall MUST wear distinguishing identification. This rule does not supersede access by watchers, official observers, and media observers in accordance with Rule 8.

[Current Rule 43.2.9 is amended and relocated to New Rule 43.6 as follows:]

43.2.9 43.6 Internal Controls for the Voting System

(a) 43.6.1 The County must enable, create, and use passwords.

(b) 43.6.2 In addition to the access controls discussed in Rule 43.2.3(e) 43.5, the county MUST change all passwords and limit access to the following areas:

(4)(A) Software. The county MUST change all software passwords once per calendar year prior to the first election. This includes any boot or startup passwords in use, as well as any administrator and user passwords and remote device passwords.
(2)(B) Hardware. The county shall MUST change all hardware passwords once per calendar year prior to the first election. This includes any encryption keys, key card tools, supervisor codes, poll worker passwords on smart cards, USB keys, tokens, and voting devices themselves as it applies to the specific system.

(3)(C) Password Management. The county shall MUST limit access to the administrative passwords to the election management software to two employees. The county shall MUST limit access to passwords for all components of the election software and hardware to two employees. The county may provide an additional ten employees with access to the administrative passwords for the software components, and an additional ten employees with access to the administrative passwords for the hardware components of the voting system. THE VOTING SYSTEM PROVIDER MAY NOT HAVE AN ADMINISTRATIVE OR APPLICATION USER/OPERATOR ACCOUNT, OR ADMINISTRATIVE ACCOUNT ACCESS TO THE ACCOUNTS.

[Language from current Rule 45.5.2.6.1(a)(vi) is amended and relocated to Rule 43.6.2]

(4)(D) Internet Access. The county must never connect or allow a connection of any voting system component to the Internet.

(5)(E) Modem Transmission. The county must never connect any component of the voting system to another device by modem except for the vote tally software as allowable by the certification of the specific device.

(6)(F) Remote sites VOTER SERVICE AND POLLING CENTERS. AT REMOTE VOTER SERVICE AND POLLING CENTERS, THE COUNTY may use modem functions of optical scanners and DREs only for the purpose of transmitting unofficial results, as permitted by the Secretary of State’s certification documents for the specific systems. A county using modem devices to transmit results shall meet the following requirements:

(A) A county may use a modem device only after all steps to close the polls are complete and summary tapes are printed, and may only use the device to transmit test data or unofficial results.

(B) The county shall not use a modem for any programming, setup, or individual ballot-casting transmissions.

(C) The county shall change the receiving telephone number for the modem transmission at least once per calendar year prior to the first election.

(D) The county may provide the telephone number of the modem receiving the transmission to no more than six employees. The
county shall not publish or print the receiving modem telephone number for any election judge. To the extent possible, the county shall program the telephone number into the device and use the device in a way that hides the display of the number from the view of election judges and voters at all times.

(7)(g) Authorized Employees. The county shall MUST include in their security plan the employees’ titles—EACH EMPLOYEE’S TITLE and the dates DATE OF CBI background checks ICHC for employees with access to any of the areas or equipment set forth in this Rule. Each county shall MUST maintain a storage facility access log that details employee name, date, and time of access to the storage facility in which the software, hardware, or components of any voting system are maintained. If access to the storage facility is controlled by use of key card or similar door access system that is capable of producing a printed paper log including the person’s name and date and time of entry, such a log shall MUST meet the requirements of this rule. [Section 24-72-305.6, C.R.S.]

43.2.4-43.7 Temperature-controlled storage. The county must maintain all components of the voting system and ballots in a temperature-controlled STORAGE environment. The county shall MUST attest to the temperature-control settings used with the following components of a voting system. Information submitted to the Secretary of State shall MUST 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 county must maintain the following required temperature settings:

(a) 43.7.1 Servers and workstations. The county shall maintain the temperature so that the maximum temperature at no time exceeds 90 degrees Fahrenheit.

(b) 43.7.2 DREs. The county shall MUST maintain the temperature at a minimum of 50 degrees Fahrenheit and a maximum of 90 degrees Fahrenheit.

(e) 43.7.3 Optical scanners. The county shall MUST maintain the temperature at a minimum of 50 degrees Fahrenheit and a maximum of 90 degrees Fahrenheit.

(d) 43.7.4 VVPAT records, PAPER BALLOTS, AND VIDEO DATA RECORDS. In addition to the requirements set forth in Rule 11, the county shall MUST maintain A DRY ENVIRONMENT AND A the temperature at a minimum of 50 degrees Fahrenheit and a maximum of 90 degrees Fahrenheit. The county shall maintain V-VPAT records in a dry environment, with storage at least 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. The county shall store V-VPAT records in a manner that prevents exposure to light, except as necessary during recounts and audits.
(e) Paper Ballots. The county shall maintain paper ballots in a dry, humidity-controlled environment. The humidity of the environment shall not exceed 80% humidity for a period of more than 24 hours. The county shall store paper ballots at least four inches above the finished floor, for a period of 25 months following the election.

(f) Video Data Records. The county shall maintain video data records in a dry, temperature-controlled environment. The humidity of the environment shall not exceed 80% humidity for a period of more than 24 hours. The county shall maintain temperature at a minimum of 50 degrees Fahrenheit and a maximum of 90 degrees Fahrenheit. The county shall store video data records at least four inches above the finished floor, for a period of 25 months following the election.

43.2.5-43.8 Security cameras or other surveillance.

43.2.3(c)(1)(C)(ii) 43.8.1 The county shall MUST maintain a log of each person who enters the ballot storage room SPECIFIED AREAS, including the person’s name, signature, and date and time of entry. If access to the ballot storage room SPECIFIED AREAS 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

(a) 43.8.2 Unless otherwise instructed, the county shall MUST make video security surveillance recordings of specified areas beginning at least 60 days prior to the election and continuing through at least 30 days after the election, unless there is a recount or contest. IF A RECOUNT OR CONTEST OCCURS, THE RECORDING MUST CONTINUE THROUGH THE CONCLUSION OF ALL SUCH ACTIVITY. The recording system shall MUST ensure that records are not written over when the system is full. The recording system shall MUST 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 MUST 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.

43.8.3 The following are the specific minimum requirements:

(4)(A) If the county has 50,000 or more registered voters, then the county shall MUST MAINTAIN A LOG AND make video security surveillance recordings of the following areas, excluding voting booths:

(A)(1) All areas in which election management software is used, including but not limited to programming, downloading memory cards, uploading memory cards, tallying results, and results reporting.

(B)(2) 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 35 days prior to the
election and continuing through at least 30 days after the election,
unless there is a recount or contest. If a recount or contest occurs,
the recording shall MUST continue through the conclusion of all
such activity.

(C)-(3) The storage area for all voting equipment.

(2)-(b) If the county has fewer than 50,000 registered voters then the county shall
MUST MAINTAIN A LOG AND make video security surveillance recordings of
all areas, excluding voting booths, in which election management software
is used, including but not limited to programming, downloading memory
cards, uploading memory cards, tallying results, and results reporting.

(b)-(c) The county must adequately and continuously light the area(s) subject to
video surveillance to provide visibility for video recording.

43.2.6-43.9 Equipment maintenance procedures. In addition to the requirements for voting
systems INVENTORY specified in Rule 11.4, the county shall MUST adhere to the following
minimum standards:

(a) 43.9.1 The county shall MUST store all equipment throughout the year with seals
over the memory card slots for each device. The county shall MUST maintain a log
of the seals used for each device consistent to the logs used for tracking Election
Day seals.

(b) 43.9.2 For equipment being sent to the vendor for offsite repairs/replacements,
the county must keep a maintenance log for the device that shall MUST contain the
following: the model number, serial number, and the type of device; the firmware
version; the software version (as applicable); the printed name and signature of
the person sending the equipment; and the date of submission to the vendor.

(e) 43.9.3 When a vendor provides on-site maintenance of equipment, vendor
personnel shall annually provide to the county a CBI or equivalent background
check for all vendor personnel that will have access to any component of the
voting system. The county must keep current CBI or equivalent background check
information on file. Additionally, an AN employee shall escort the vendor’s
representative at all times 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. [Section 24-72-305.6, C.R.S.]

(d) 43.9.4 Upon completion of any maintenance, the county shall MUST verify or
reinstate the trusted build and conduct a full acceptance test of equipment that
shall MUST, at a minimum, include the hardware diagnostics test, as indicated in
Rule 11, and conduct a mock election in which an employee(s) shall MUST cast a
minimum of five ballots on the device to ensure tabulation of votes is working
correctly. The county shall MUST maintain all documentation of the results of the
acceptance testing on file with the specific device.
43.9.5 The Secretary of State will annually inspect county maintenance records on a randomly selected basis.

43.2.7-43.10 Transportation of equipment, memory cards, ballot boxes, and ballots.

(a) 43.10.1 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. If there is any evidence of possible tampering with a seal, or if the serial numbers do not match those listed in the chain-of-custody log, the county clerk must be immediately notified and must follow the procedures specific to the incident as described in Rule 43.15.1. While the method of transportation of equipment may vary, the following standards shall apply when transporting voting equipment to the voting location:

(1) (A) Transportation by county personnel. County personnel shall display a badge or other identification provided by the County. Two employee signatures and date of employees are 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 employees or election judges shall verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact and that the serial numbers on the seals match the logged serial numbers. If there is any evidence of possible tampering with a seal, or if the serial numbers do not match those listed in the chain-of-custody log, they shall immediately notify the county clerk and recorder who shall follow the procedures specific to the incident as described in 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 chain-of-custody log for the device. The election judge receiving the equipment shall request two election judges at the voting location to inspect the device and to sign and date the chain-of-custody log indicating that all seals are intact and that the serial numbers on the seals match 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 match those listed in the chain of custody log, they shall immediately notify the county clerk and recorder who shall follow the procedures specific to the incident as described in Rule 43.2.11.

(3) (C) Transportation by contract. A county electing to contract the delivery of equipment to remote voting locations shall perform an CBI background checks on each of the specific individuals who will be delivering the equipment. Two employees or election judges shall verify, sign, and date the chain-of-custody log upon release of the equipment to the individual(s) delivering the equipment. Two—other
employees or election judges shall verify, sign, and date the chain-of-custody log after delivery of the equipment, 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 match those listed in the chain-of-custody log, they shall immediately notify the county clerk and recorder who shall follow the procedures specific to the incident as described in Rule 43.2.11.

(Section 24-72-305.6, C.R.S.)

(b) 43.10.2 Standards for transporting voting equipment to and from the voting location:

(4) (A) Required procedures if memory cards or cartridges are removed from voting devices at remote voting locations:

(A) (1) Before removing a memory card or cartridge, two election judges shall inspect and verify that all seals on the device are intact and that the serial numbers on the seals match those listed on the chain-of-custody log. Both election judges shall sign and date the 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 match those listed in the chain-of-custody log, they shall immediately notify the county clerk and recorder who shall follow the procedures specific to the incident as described in Rule 43.2.11.

(B) (2) Election judges shall place the memory cards or cartridges in a sealable transfer case and must seal the case with at least one seal. The election judges shall maintain a chain-of-custody log for the transfer case of the memory cards or cartridges.

(C) (3) Election judges shall place new seals over the empty memory card/cartridge slot and/or door and document the seal numbers used.

(D) (4) At least two county personnel or election judges shall accompany the transfer case containing the memory cards/cartridges to the drop-off PROCESSING location. The election judges who receive the equipment must verify, and indicate by signing and dating the chain-of-custody log, that the seals are intact and seal serial numbers match those listed in the log. If there is any evidence of possible tampering with a seal, or if the serial numbers do not match those listed in the chain-of-custody log, 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 Rule 43.2.11.
(5) County personnel or election judges transporting secured voting
equipment must maintain chain-of-custody logs. If there is any
evidence of possible tampering with a seal, or if the serial numbers
do not match those listed in the chain-of-custody log, they shall
immediately notify the county clerk and recorder who shall follow
the procedures specific to the incident as described in Rule
43.2.11.

(2) (b) Required procedures if devices are delivered with memory
cards/cartridges intact:

(A) (1) Two county personnel or election judges shall—MUST verify that all
seals are intact at the close of polls. Election judges shall—MUST
sign and date the 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 match those listed in the chain of custody
log, they shall immediately notify the county clerk and recorder
who shall follow the procedures specific to the incident as
described in Rule 43.2.11.

(B) (2) At least two county personnel or election judges shall—MUST
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
match those listed in the chain of custody log, they shall
immediately notify the county clerk and recorder who shall follow
the procedures specific to the incident as described in Rule
43.2.11. THE PERSON RECEIVING THE EQUIPMENT MUST VERIFY THE
SEALS AND SIGN AND DATE THE LOGS.

(C) (3) Upon confirmation that the seals are intact and bear the correct
numbers, election judges OR THE COUNTY shall—MUST remove and
upload the memory cards/cartridges into the central count system.

(D) (4) To secure the equipment, election judges shall—MUST place a
tamper-evident seal over the memory card slot and update the
chain-of-custody log to reflect the new seal number(s).

(e) 43.10.3 Required procedures for transportation of ballot boxes:

(A) Election judges shall—MUST seal all ballot boxes that contain voted ballots
so that no person can access the ballots without breaking a seal. The
election judges shall—MUST record all seals in the chain-of-custody log and
two election judges shall—MUST verify, and indicate by signing and dating
the log, that the required seals are intact.
(2) (B) Two county personnel or election judges shall accompany all ballot boxes that contain voted ballots at all times, except when the ballot box is located in a vault or secure physical location.

(3) (C) The ballot box exchange requirements of section 1-7-305, C.R.S., are met if a chain-in-custody log is completed for each ballot box.

43.11 ELECTRONIC POLLBOOKS.

38.3.1 43.11.1 The designated election official shall establish written security procedures covering:

(A) The transference of teleprocessing information;

38.3.2 (B) Such procedures shall include security covering:

38.3.3 43.11.2 The county shall submit in the security plan the system data transfer requirements to completely process a single voter record. This shall include at a minimum the following:

a. (A) The data stream information on both send and receiving data for all points of the transaction until the transaction is complete;

b. (B) Information on all points where the connection is closed and the data stream released between the remote computer and the server; and

c. (C) The proposed method of securing transmissions across public networks.

38.5.4 43.11.3 The county shall submit in the security plan a detailed list of all vote centers, with a proposed number of workstations connecting to the database and the proposed connection (including bandwidth and security) for each location.

[Current Rule 43.2.8 is amended, including amended current Rules 38.3.3-38.3.5, as follows]

43.2.8 43.12 Contingency plans.

(a) 43.12.1 Emergency. The county must develop emergency contingency plans for voting equipment and voting locations in accordance with Rule 45.

(i) All remote devices used in an election shall have sufficient battery backup for at least two 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. The use of third-party battery backup systems also meets this requirement.

(2) 43.12.2 In the event of a serious or catastrophic equipment failure, or when equipment is removed from service at one or more polling locations, or there is not adequate backup equipment to meet the requirements of section 1-5-501, C.R.S., the county clerk and recorder shall notify the Secretary of State that the county is using provisional ballots or mail-in ballots as an emergency voting method.

(b) A security plan must contain a section entitled “contingency plan” that includes 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 the county contingency plans and evacuation procedures must address emergency situations including fire, severe weather, bomb threat, civil unrest, electrical blackout, equipment failure, and any other emergency situations 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.

38.3.3 43.12.4 Such procedures shall include contingency procedures for network and power failure. Such procedures shall at a minimum include procedures the county must develop procedures to address all single-point failures of SCORE continuity, including:

a. network failure,

b. power failure that lasts less than one (1) hour, and

e. Power failure that lasts more than one (1) hour.

38.3.4 Acceptable alternatives for addressing such failures include either:

a. A paper backup of the pollbook with the minimum information required to verify a voter’s eligibility; or

b. A sufficient number of computers per vote center to ensure that the voter check-in continues in an efficient manner. The computers shall have the ability to function on batteries or an external power source for up to two (2) hours. In addition, each computer shall
have an electronic backup of the current pollbook in one (1) of the following formats:

i. —— A Portable Document File (PDF);

ii. —— A spreadsheet that is limited to sixty-four thousand (64,000) lines if in Excel; or

iii. —— A database with a basic look-up interface.

38.3.5 43.12.5 In addition to acceptable backup pollbook procedures, the security procedures shall address contingency procedures to protect against activities such as voting twice, including but not limited to the use of an affidavit that the voter has not and will not cast another ballot.

[Current Rule 43.2.9 is amended and relocated to New Rule 43.6]

44.6.43.13 Procedures for Voter Verifiable Paper Audit Trail (V-VPAT). The following requirements apply only to DREs with a VVPAT.

44.6.143.13.1 Security. 44.6.1.1 —— The V-VPAT—VVPAT record is considered an official record of the election, pursuant to IN ACCORDANCE WITH section 1-5-802, C.R.S. All security procedures related to election ballots shall MUST apply to V-VPAT—VVPAT records.

44.6.1.2(A) The housing unit for any V-VPAT—VVPAT record to be used in the election shall MUST be sealed and secured prior to any votes being cast for the election. Documentation of the seal number(s) must be maintained and noted prior to voting, and at the conclusion of voting. (a) Election judges shall MUST attest to the V-VPAT—VVPAT record having no votes included on the paper record prior to the start of voting, and prior to the installation or replacement of a new V-VPAT—VVPAT record. DOCUMENTATION OF THE SEAL NUMBER(S) MUST BE MAINTAINED AND NOTED PRIOR TO VOTING, AND AT THE CONCLUSION OF VOTING.

44.6.1.3(B) If a DRE with V-VPAT—VVPAT is used during early voting, the seal number(s) must be recorded at the beginning and end of each voting day.

44.6.1.4(C) At the close of the polls, the V-VPAT—VVPAT records will be transferred to the central ELECTION office in the same manner as any paper ballots. In the absence of paper ballots, the V-VPAT—VVPAT records will be transferred to the central ELECTION office in the same manner as any memory cards containing electronic ballots.

44.6.243.13.2 Anonymity. 44.6.2.1 —— The Election Official DESIGNATED ELECTION OFFICIAL shall put IMPLEMENT measures in place to protect the anonymity of
voters choosing to vote on DREs during the voting periods. These measures shall include:

(A) MEASURES TO PROTECT THE ANONYMITY MAY INCLUDE:

(a) Encouraging poll workers to personally vote on DREs when possible to ensure more than one vote will be cast on the device.

(b) (1) Appropriate marking in Poll Book or other voting list indicating voters’ choice to vote on DRE with the words: “Voted DRE”, or similar in place of paper ballot information. No record may be kept indicating the order in which people voted on the DRE, or which V-VPAT-VVPAT record is associated with the voter.

(e)(2) When more than one DRE is available at a voting location, the voter shall be given the choice as to which DRE they would like to vote on, to the extent practical.

(d) Encouraging or allowing any and all voters the opportunity to vote on a DRE if desired.

11.6.2.2 (b) Any report or export (electronic or paper based) generated from an electronic pollbook shall remove the date/time stamp from the record and not use this field as a sort method. Any assignment of Record IDs, Key ID, or Serial Number stored in the database of votes shall be randomly assigned.

11.6.2.3 Any Pollbook, electronic, paper or otherwise shall not be exposed to the same people at the same place who have exposure to the V-VPAT VVPAT records.

(c) ELECTION JUDGES MAY NOT ACCESS VVPAT RECORDS AT THE TIME OF VOTING.

11.6.2.4 The Examination of the V-VPAT-VVPAT record shall always be done PERFORMED by at least two witness ELECTION JUDGES.

11.6.3.1 Storage. The storage of the V-VPAT-VVPAT records must be consistent with storage of paper ballots pursuant to section 1-7-802, C.R.S.

11.6.3.2 (a) Individual spools containing V-VPAT-VVPAT records must contain the following catalog information affixed to the spool:

(a) (1) Date and name of election;

(b) (2) Name of voting location;
(e)(3) Date(s) and time(s) of voting;

(d)(4) Machine serial number of DRE associated with the record; and

(e)(5) Number of spools associated with this machine for this election (i.e. “Spool 1 of 1”, or “Spool 1 of 2”, etc.).

11.6.3.3 (B) Light sensitive storage containers shall MUST be used for the 25 month storage period to ensure the integrity of the V-VPAT VVPAT paper record. Containers shall MUST be sealed, with record of the seal numbers maintained on file and signed by two elections officials JUDGES.

11.6.3.4 (C) A master catalog shall MUST be maintained for the election containing the complete total number of V-VPAT VVPAT spools used in the election.

[Current Rule 11.6 is amended and relocated to New Rule 43.13. Amendments are shown above.]

43.2.10 43.14 Security training for election judges. (a)—The county shall MUST include in their security plan the details of their security training for their election judges IN ACCORDANCE WITH RULE XX. The county must address the anticipated time of training, location of training, and number of election judges receiving the security training, as it applies to the following requirements:

(4) (A) The county shall MUST conduct a separate training module for field technicians and election judges 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 MUST include the following components:

(A)(1) Proper application and verification of seals and chain-of-custody logs;

(B)(2) 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)(3) Ensuring privacy in voting booths;

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

(E)(4) V-VPAT VVPAT requirements;

(F)(5) Chain-of-custody requirements for voting equipment, memory cards/cartridges, and other election materials;
(G) Ballot security;

(H) Voter anonymity; and

(I) Recognition and reporting of security incidents.

43.2.11 43.15 Remedies.

(a) If a seal is broken, or if there is a discrepancy in a chain-of-custody log, the election judges shall immediately notify the county clerk and recorder, who shall investigate, complete and submit to the Secretary of State an internal incident report, and follow the appropriate remedy as indicated in this rule or as directed by the Secretary of State.

(b) 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. Any unit involved must undergo the reinstatement or verification of the trusted build, in accordance with State instructions. The following remedial actions are required if a device was tampered with. (The county clerk and recorder may determine additional requirements based on the details of the incident report):

(A) The county or Secretary of State must reinstate or verify the trusted build. For instances where the county can display, verify, or print the trusted build hash value (MD5 or SHA-1) of the firmware or software, the election official shall document and verify that the hash value matches the documented alphanumeric string associated with the trusted build for the software or firmware of that device.

(B) If the evidence indicates that the tampering discrepancy occurred prior to the start of voting:

(1) The election judges shall seal the device and securely deliver it to the county clerk and recorder.

(2) The county clerk and recorder or his or her designee shall remove and secure the memory card following the procedures in Rule 43.2.2(d). 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 or the Secretary of State must install a new, secure memory card into the device, conduct a hardware diagnostics test as prescribed in Rule 11, and proceed to conduct an acceptance test on the machine.
in full election mode, casting at least 25 ballots on the device. The county shall MUST maintain on file all documentation of testing and chain of custody for each specific device.

(C)(3) The county shall MUST complete the necessary seal process and documentation to re-establish the chain of custody for the device and new memory card.

(D)(4) The county shall MUST set the machine to election mode ready for a zero report.

(E) Repealed.

(D)(C) If the evidence indicates that the tampering DISCREPANCY occurred after votes were cast on the device but before the close of polls:

(H)(1) The county MAY NOT CONTINUE TO USE THE MACHINE UNTIL VERIFICATION OR REINSTALLATION OF TRUSTED BUILD AND ACCEPTANCE TESTING IS COMPLETE. The county shall MUST set the machine to election mode ready for a zero report BEFORE RESUMING VOTING ON THE DEVICE.

(A)(2) The election judges shall MUST seal the device and securely deliver it to the county clerk and recorder.

(B)(3) The county clerk and recorder or his or her designee shall MUST close the election on that device, and perform a complete manual verification of the paper ballots (or VVPAT records) to the summary tape printed on the device that represents the record of votes on the memory card.

(C)(4) If the totals do not match then only the paper record will be accepted as the official results for that device. The county clerk and recorder shall MUST re-seal and secure the device and immediately report the discrepancy to the Secretary of State. The county must not use the device for the remainder of the election unless the trusted build is reinstated.

(D)(5) If the totals match, the county may upload the memory card into the tally software at the close of polls.

(E)(6) After verifying the totals, the county shall MUST secure the paper records and memory card with seals and a chain-of-custody log.

(F) The county shall place a new and secure memory card 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. The county shall maintain on file all documentation of testing and chain of custody for the device.

(G)(7) The county shall MUST complete the necessary seal process and documentation to establish the chain of custody for the device and memory card.

(H) The county shall set the machine to election mode ready for a zero report.

[Current Rule 43.2.11(a)(3)(H) is amended and moved to 43.15(c)(1) above]

(I)(8) At the conclusion of the election PRIOR TO CERTIFYING ELECTION RESULTS, the county shall MUST conduct a full (all races) post-election audit on the device and report results 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) Repealed.

(4) If the evidence indicates that the tampering occurred after the close of polls:

(A) The election judges shall seal the device and securely deliver it to the county clerk and recorder.

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

(C) If the totals do not match then only the paper record will be accepted as the official results for that device. The county clerk and recorder shall re-seal and secure the device and immediately report the discrepancy to the Secretary of State. The county must not use the device for the remainder of the election unless trusted build is reinstalled.

(D) If the totals match, the county may upload the memory card into the tally software at the close of polls.

(E) After verifying the totals, the county shall secure the paper records and memory card with seals and a chain-of-custody log.

(F) 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 and complete the necessary seal process and documentation to establish the chain of custody for the device.

(G) During the canvass process, the county shall conduct a full (all races) post-election audit on the device and report results 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) Repealed.

(e) 43.15.3 The county shall—MUST make all documentation related to the voting system and for every device used in the election available for Secretary of State inspection.

43.2.12 The county shall—MUST submit any additional physical security procedures not discussed in this rule to the Secretary of State for approval prior to the election.

43.3 The county shall submit with the security plan sample copies of all referenced forms, schedules, logs, and checklists.

[Current Rule 43.3 is moved to Rule 43.3.6]

43.4 Amendments and review of security plans.

43.4.1 43.16.1 If no changes have occurred since the last security plan was filed, THEN the county shall—MUST file a statement to that effect.

43.4.2 43.16.2 The county shall—MUST clearly identify and describe any revisions to a previously filed security plan.

43.4.3 43.16.3 The county may change the security plan within 60 days of an election as a result of an emergency situation or other unforeseen circumstance. The county must document the changes and file the 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 Secretary will notify the county that the security plan or revisions are temporarily approved until the review is complete.

43.5 43.17 Lease, LOAN, OR RENTAL OF ELECTION EQUIPMENT. 43.5.1—Nothing in this rule requires a county clerk to lease, loan, or rent any election equipment to any municipality, special district or other local jurisdiction.

43.5.2 43.17.1 A county clerk who—THAT 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—MUST follow at least one of the following procedures in order to maintain or reestablish an acceptable chain of custody
CHAIN-OF-CUSTODY and appropriate documentation in accordance with Rule 43.2.1 43.3.

43.5.3 43.17.2 Upon return of the certified voting equipment to the county clerk and recorder, the county clerk is required to verify the trusted build, in accordance with State instructions, if the documentation and chain of custody—CHAIN-OF-CUSTODY does not support the proper maintenance of the trusted build software and chain of custody—THEN THE COUNTY MUST REINSTATE OR VERIFY THE TRUSTED BUILD BEFORE USING THE EQUIPMENT.

(a) 43.17.3 After the local jurisdiction returns the certified equipment to the county clerk, the county clerk must reinstate or verify the trusted build in accordance with Rule 43 before the equipment is used in any primary, general, congressional vacancy, statewide ballot issue (including recall), or special election conducted by the county clerk. TO REINSTATE OR VERIFY THE TRUSTED BUILD, THE COUNTY MUST IMPLEMENT ONE OF THE FOLLOWING PROCEDURES:

(b)(A) The county clerk or their deputized representative shall MUST:

(1) Deliver the certified equipment to the jurisdiction;

(2) Witness and document the installation of the memory card(s) or cartridge(s) used by the jurisdiction;

(3) Place one or more secure and numbered seals on the voting equipment in accordance with Rule 43.2.2—43.4. 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 MUST witness and document the removal and proper resealing of the memory card or cartridge; and

(4) Upon return of the equipment to the county clerk and recorder, the county clerk shall MUST verify, and indicate by signing and dating the chain-of-custody log, that all seals are intact. If any seal is damaged or removed, the county clerk shall MUST REINSTATE or verify the trusted build in accordance with this Rule 43.

(c)(B) The county clerk and recorder shall MUST designate and station deputized county staff with the loaned certified equipment at all times while the equipment is under control of the designated election official. The deputized county staff must maintain physical custody of the certified equipment at all times to ensure that no unauthorized access occurs.

(d)(C) In accordance with section 1-5-605.5, C.R.S., the county clerk shall MUST appoint the designated election official as a deputy for the purposes of
supervising the certified voting equipment. The designated election official shall MUST:

(1) 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) Affirm that the use of the certified voting equipment is conducted in accordance with this Rule 43 and the specific Conditions for Use of the certified voting equipment; and

(3) Agree to maintain all chain-of-custody logs for the voting device(s).

43.5.3 Upon return of the certified voting equipment to the county clerk and recorder, the county clerk is required to verify the trusted build, in accordance with State instructions, if the documentation and chain of custody does not support the proper maintenance of the trusted build software and chain of custody.

[Current Rule 43.5.3 is amended and moved to New Rule 43.18.2]

43.18 BALLOT ON DEMAND

43.18.1 THE COUNTY MUST USE THE LAPTOP FOR BALLOT ON DEMAND PURPOSES ONLY.

43.18.2 SOFTWARE ACCESS, SECURITY, AND STORAGE.

(A) THE COUNTY MUST CHANGE ALL WINDOWS AND BALLOT ON DEMAND APPLICATION PASSWORDS AT LEAST ONCE PER CALENDAR YEAR.

(B) ONLY THE COUNTY, ELECTION JUDGES, SECRETARY OF STATE STAFF, OR AUTHORIZED VENDOR REPRESENTATIVES MAY OPERATE THE BALLOT ON DEMAND SYSTEM.

(C) THE COUNTY MAY CONNECT THE BALLOT ON DEMAND LAPTOP TO AN EXTERNAL NETWORK FOR THE PURPOSE OF CONNECTING TO SCORE ONLY IF THE COUNTY MAINTAINS CURRENT VIRUS PROTECTION AND IMPLEMENTS FIREWALLS TO PREVENT UNAUTHORIZED ACCESS.

(D) THE COUNTY MUST STORE THE LAPTOP(S) AND UNUSED PAPER BALLOT STOCK IN A LOCKED STORAGE AREA WHEN THE PRINTER IS NOT IN USE.

43.18.3 BALLOT RECONCILIATION.

(A) THE COUNTY MUST RECONCILE BALLOTS PRINTED ON DEMAND IN ACCORDANCE WITH RULES 41.4 AND 41.5.
(B) THE COUNTY MUST MAINTAIN DAMAGED, MISPRINTED, OR UNUSABLE BALLOTS AS ELECTION RECORDS.

Rule 44. RESERVED

Rule 45. Rules Concerning Voting System Standards for Certification

45.1 Definitions. The following definitions apply to their use in this rule only, unless otherwise stated.

45.1.1 “Audio ballot” means a voter interface containing the list of all candidates, ballot issues, and ballot questions upon which an eligible elector is entitled to vote in an election. It also provides the voter with audio stimuli and allows the voter to communicate voting intent to the voting system through vocalization or physical actions.

45.1.2 “Audit log” means a system-generated record, in printed and/or electronic format, providing a record of activities and events relevant to initializing election software and hardware, the identification of files containing election parameters, initializing the tabulation process, processing voted ballots and terminating the tabulation process.

45.1.3 “Ballot image” means a corresponding representation in electronic form of the marks or vote positions of a cast ballot that are captured by a direct-recording electronic voting device DRE.

45.1.4 “Ballot Marking Device” or “BMD” means a device that uses electronic technology to:

(A) MARK AN OPTICAL SCAN BALLOT AT VOTER DIRECTION,

(B) INTERPRET THE BALLOT SELECTIONS,

(C) COMMUNICATE THE INTERPRETATION FOR VOTER VERIFICATION, AND THEN

(D) PRINT A VOTER-VERIFIED BALLOT.

A BMD INTEGRATES COMPONENTS SUCH AS AN OPTICAL SCANNER, PRINTER, TOUCH-SCREEN MONITOR, AND A NAVIGATIONAL KEYPAD.

45.1.5 “Ballot style” means a specific ballot layout or content for an election. The ballot style is the presentation of the unique combination of contests and candidates for which the voter is eligible to vote. It includes the order of contests and candidates, the list of ballot positions for each contest, and the binding of candidate names to ballot positions within the presentation. Multiple precincts may use a single ballot style. Multiple styles may appear in a single precinct where voters are split between two or more districts or other categories defining voter eligibility for particular contests and candidates.
45.1.5 “Closed network” means a network structure in which devices are not connected to the internet or other office automation networks, except as allowable under THIS Rule 45.5.2.7.45.

45.1.6 “Communications devices” means devices that may be incorporated in, or attached to, components of the voting system for the purpose of transmitting tabulation data between components or to another data processing system, printing system or display device.

45.1.7 “DRE” means a direct recording electronic voting device. A DRE is a voting device that records votes by means of a ballot display OR AN AUDIO BALLOT provided with mechanical or electro-optical components or an audio ballot that can be activated by the voter, processes data by means of a computer SOFTWARE program and 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.

45.1.8 “EAC” means the United States Election Assistance Commission.

45.1.9 “Election management system” includes, but is not limited to, the ballot definition subsystem and the election reporting subsystem. The election management system may provide utilities for other election administration tasks, including maintaining equipment inventories, estimating ballot printing needs and maintaining information on polling places.

45.1.10 “Election media” means any device including a cartridge, card, memory device or hard drive used in a voting system for the purposes of programming ballot image data (ballot or card styles), recording voting results from electronic vote tabulating equipment or any other data storage required by the voting system for a particular election function. The election management system typically downloads ballot style information to the election media and uploads results and ballot images from the election media.

45.1.11 “Equipment” or “device” means a complete, AND inclusive term to represent all items submitted for certification by the voting system provider. This can include, but is not limited to, any voting device, accessory to voting device, DRE, touch screen voting device, card programming device, software and hardware. “Equipment” may also mean a complete end to end voting system solution.

45.1.12 “MODIFICATION” MEANS A REVISION OR A NEW RELEASE OF AN ELECTRONIC OR ELECTROMECHANICAL VOTING SYSTEM.

45.1.13 “Remote site” means any physical location identified by a designated election official as a location where the jurisdiction shall conduct the casting of ballots for a given election. A remote site includes, but is not limited to,
locations such as precinct polling places, vote centers, early voting sites and mail-
in ballot counting sites.

45.1.14 “Removable Storage Media” “REMOVABLE STORAGE MEDIA” means storage devices that can be removed from the system and transported to another location for readout and report generation. Examples of removable storage media include, but are not limited to, programmable read-only memory (PROM), random access memory (RAM) with battery backup, thumb drives, magnetic media and optical media.

45.1.15 “Secretary of State” within the context of this rule, means the Colorado Secretary of State and his or her designated agents including employees, contractors and volunteers.

45.1.16 “Security” means the ability of a voting system to protect election information and election system resources with respect to confidentiality, integrity and availability.

45.1.17 “Split Precinct” “SPLIT PRECINCT” means a precinct that has a geographical divide between one or more political jurisdictions which results in each jurisdiction within the precinct to be assigned different ballot styles for a specific election.

45.1.18 “Test Log” or “Test Records” “TEST LOG” OR “TEST RECORDS” means the documentation of certification testing and processes. This documentation may include, but is not limited to, certification testing reports, test plans, requirements matrices, photographs, written notes, video and/or audio recordings.

45.1.19 “Trusted Build” “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 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.

45.1.20 “VOTING SYSTEM” MEANS:

(A) THE TOTAL COMBINATION OF MECHANICAL, ELECTROMECHANICAL, OR ELECTRONIC EQUIPMENT (INCLUDING THE SOFTWARE, FIRMWARE, AND DOCUMENTATION REQUIRED TO PROGRAM, CONTROL, AND SUPPORT THE EQUIPMENT) THAT IS USED TO:

(1) DEFINE BALLOTS;

(2) CAST AND COUNT VOTES;
(3) REPORT OR DISPLAY ELECTION RESULTS; AND

(4) MAINTAIN AND PRODUCE ANY AUDIT TRAIL INFORMATION; AND

(B) THE PRACTICES AND ASSOCIATED DOCUMENTATION USED TO:

(1) IDENTIFY SYSTEM COMPONENTS AND VERSIONS OF SUCH COMPONENTS;

(2) TEST THE SYSTEM DURING ITS DEVELOPMENT AND MAINTENANCE;

(3) MAINTAIN RECORDS OF SYSTEM ERRORS AND DEFECTS;

(4) DETERMINE SPECIFIC SYSTEM CHANGES TO BE MADE TO A SYSTEM AFTER THE INITIAL QUALIFICATION OF THE SYSTEM; AND

(5) MAKE AVAILABLE ANY MATERIALS TO THE VOTER (SUCH AS NOTICES, INSTRUCTIONS, FORMS, OR PAPER BALLOTS).

45.1.19 45.1.21 “Voting System Test Laboratory” or “VSTL” means a “Federally Accredited Laboratory” “VOTING SYSTEM TEST LABORATORY” or “VSTL” means a “FEDERALLY ACCREDITED LABORATORY”, as defined in section 1-1-104(16.5), C.R.S., which is accredited by the EAC to conduct certification testing for voting systems.

45.5.2.9.1-45.1.22 V-VPAT shall refer to a Voter verified “VOTER-VERIFIED PAPER AUDIT TRAIL” or “VVPAT” means a device capable of producing a voter-verified paper record as defined in section 1-1-104(50.6)(a), C.R.S.

45.2 Introduction

45.2.1 Definition of voting system for certification purposes

45.2.1.1 The definition of a voting system for the purposes of this rule shall be as the term is defined in HAVA Section 301(b). For Colorado purposes, no single component of a voting system, or device, meets the definition of a voting system except that nothing in this rule shall be interpreted to require the testing of an entire modified system if the Secretary of State determines pursuant to IN ACCORDANCE WITH section 1-5-618, C.R.S., that a modification to any certified voting system requires testing for security and accuracy. only—ONLY the modification shall be required to be tested to ensure compliance with this Rule 45.

45.2.1.2 Sufficient components shall be assembled to create a configuration that allows the system or modification as a whole to meet the requirements as described for a voting system in this rule.

45.2.3 THE CERTIFICATION OF A VOTING SYSTEM SHALL NOT BE INTERPRETED AS A REQUIREMENT THAT A COUNTY PURCHASE OR LEASE ALL OF THE COMPONENTS OF
THE VOTING SYSTEM. COUNTIES MAY CHOOSE TO CONFIGURE AND USE A SUBSET OF
THE CERTIFIED VOTING SYSTEM AND MAY USE THE SERVICES OF A VENDOR OR
THIRD PARTY TO PROVIDE BALLOT DEFINITION AND ELECTION PROGRAMMING OF
MEMORY CARDS. COUNTIES ARE NOT REQUIRED TO USE A PAPER BALLOT
TABULATION DEVICE IF THEY CHOOSE TO MANUALLY TABULATE THE ELECTION
RESULTS.

45.2.2 Authority

45.2.2.1 Pursuant to Articles 5 and 7 of Title 1, C.R.S., the Secretary of
State is expressly authorized to adopt this rule.

45.2.3 Documents Incorporated by Reference

45.2.3.1 All documents incorporated by reference in this Rule 45 do not
include any later amendments or editions of those documents.

45.2.3.2 All documents incorporated by reference in this Rule 45 may be
viewed on the “Voting Systems” page of the “Elections Center” on the
Secretary of State’s website at www.sos.state.co.us, or by contacting the
Secretary of State Voting Equipment Certification Program/1700
Broadway–Suite 200/Denver, CO 80290.

45.3 Certification Process Overview and Timeline

45.3.1 The voting system shall be considered as a unit, and all components of such
system shall be tested at once, unless the circumstances necessitate otherwise.
Any change made to individual components of a voting system shall require the
entire voting system to be recertified in accordance with this rule unless the
change is a modification that can be approved under the provisions of section 1-5-
618(1.5), C.R.S.

45.3.2 For a voting system to be certified, the voting system provider shall successfully
complete all phases of the certification process, to include submitting a complete
application, a review of the documentation to evaluate whether the system meets
the requirements of this rule, a public demonstration of the system, functional
testing of the voting system to demonstrate substantial compliance with the
requirements of this rule and Colorado Election Code as well as any additional
testing that is deemed necessary by the Secretary of State. THE CERTIFICATION
PROCESS INCLUDES: SUBMISSION OF A COMPLETE APPLICATION, A DOCUMENTATION
REVIEW, A PUBLIC DEMONSTRATION OF THE SYSTEM, AND FUNCTIONAL TESTING.

45.3.3 The flow of each phase of certification is as follows:

(a) Phase I – Voting. THE VOTING system provider submits MUST SUBMIT an
application and all documentation required in Rule 45.4. The Secretary of
State reviews WILL REVIEW the application APPLICATION and informs
INFORM the voting system provider whether or not the application is
complete. If the application is complete, the Secretary of State makes arrangements with the voting system provider for a public demonstration.

If the application is incomplete, the Secretary of State shall identify the deficiencies and the voting system provider will have 30 days to remedy the deficiencies and make the application complete. When the application is complete, the Secretary of State will make arrangements with the voting system provider for a public demonstration.

(b) Phase II – The Secretary of State reviews the submitted documentation, conducts the review of VSTL reports from previous testing, and or—evaluations provided by another State under Rule 45.5.1.3, prepares a certification test plan for the system and presents the test plan to the voting system provider other states.

(c) Phase III – The Secretary of State will prepare a certification test plan. If a VSTL is contracted to test the voting system, the VSTL will work with the Secretary of State to prepare a certification test plan. The certification test plan will be presented to the voting system provider for review prior to the start of functional testing.

(d)-(E) Phase IV— Upon receipt of the voting system provider’s agreement to the certification test plan, the Secretary of State performs or the VSTL will perform the functional tests.

(d)-(E) Phase IV— The Secretary of State reviews the results of the functional tests and decides—determine whether to certify or not to certify the voting system substantially meets the requirements for certification. Within 30 days of this decision to certify or not certify the voting system, the certification test report for the voting system shall be posted on the Secretary of State’s website.

45.6.3-45.3.4 The Secretary of State shall certify voting systems that substantially comply with the requirements in this Rule 45, Colorado Election Code, and any additional testing that is deemed necessary by the Secretary of State.

45.4 Application Procedure

45.4.1 Any voting system provider may apply to the Secretary of State for certification at any time.

45.4.2 A voting system provider that submits—desires to submit a voting system for certification shall complete the Secretary of State’s “Application for Certification of Voting System” which is available on the Secretary of State’s website.

45.4.3 The Secretary of State, in accordance with section 24-21-104(1)(a), C.R.S., shall charge the voting system provider all direct and indirect costs associated with the
testing of a voting system submitted for certification. The Secretary of State shall provide, upon request, an estimate of costs for certification testing at the conclusion of Phase II evaluation. Prior to the commencement of functional testing. In order to begin functional testing, the voting system provider shall provide a written approval of the cost estimate. All costs shall be paid in full prior to the issuance of a final determination by the Secretary of State.

45.4.4 Along with the application, the voting system provider shall submit all documentation required in this Rule 45 in electronic format. The requirements include documentation necessary for the identification of the full system configuration submitted for certification. Documentation shall include information that defines the voting system design, method of operation and related resources. It shall also include a system overview and documentation of the voting system’s functionality, accessibility, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures and personnel deployment and training requirements. In addition, the documentation submitted shall include the voting system provider’s configuration management plan and quality assurance program.

45.4.5 Electronic copies of documentation are preferred and shall be submitted in lieu of a hard copy when possible.

45.4.6 45.4.5 The vendor shall identify any material it asserts is exempt from public disclosure under the Colorado Open Records Act, section 24-72-204, et. seq., C.R.S., together with a citation to the specific grounds for exemption. The request shall be made prior to the start of Phase III-IV of the certification process.

45.4.7 If the EAC has established a trusted build for the system submitted for certification, the trusted build shall be provided by the EAC. The voting system provider shall execute and submit to the EAC any necessary releases for the EAC to provide the same and provide the Secretary of State with a copy of such executed releases. The voting system provider shall pay directly to the EAC any cost associated with same. In addition, the voting system provider shall submit all documentation and instructions necessary for the creation and guided installation of files contained in the trusted build which will be created at the start of functional testing and will be the model tested. The Secretary of State reserves the right to add additional instructions or guidance for the use of the trusted build when initiating the chain of custody process for a jurisdiction using the specified equipment.

45.4.8 45.4.6 If the EAC does not have a trusted build for the voting system submitted for certification, the voting system provider shall coordinate with the Secretary of State for the establishment of the trusted build. The voting system provider shall submit all documentation and instructions necessary for the creation and guided installation of files contained in the trusted build which will be created at the start of functional testing and will be the model tested. At a minimum, this trusted build shall
include a compilation of files placed on write-once media for which the Secretary of State has observed the chain of evidence from the time of source code compilation through delivery, and an established hash file distributed from a VSTL or the National Software Reference Library to compare federally certified versions. All or any part of the trusted build disks may be encrypted. If applicable, they should all be labeled as proprietary information and with identification of the voting system provider’s name and release version based on the voting system provider’s release instructions. All or any part of the

45.4.9 45.4.7 All materials submitted to the Secretary of State shall remain in the custody of the Secretary of State during the life of the certification and for 25 months after the last election in which the system is used with the exception of any equipment provided by the voting system provider for the purposes of testing, as follows:

(A) FOR CERTIFIED SYSTEMS, UNTIL THE CERTIFICATION IS PERMANENTLY REVOKED, OR UNTIL NO COMPONENTS OF THE CERTIFIED SYSTEM ARE USED IN THE STATE OF COLORADO; AND

(B) FOR SYSTEMS THAT ARE NOT CERTIFIED, A PERIOD OF 25 MONTHS.

45.4.10 45.4.8 In addition to the application and the documentation specified above, the Secretary of State may request additional information from the applicant, as deemed necessary.

45.5 Voting System Standards

45.5.1 Federal Standards

45.5.1.1 45.5.1 All voting systems shall meet the voting system standards pursuant to section 1-5-601.5, C.R.S., and Secretary of State Rule 37.3-2002 VOTING SYSTEM STANDARDS.

45.5.1.2 45.5.2 All voting system software, hardware and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not limited to, (a) the Help America Vote Act, (b) the Americans with Disabilities Act and (c) the Federal Rehabilitation Act. The voting system provider shall explicitly acknowledge that their proposed software, hardware and firmware are all in compliance with the relevant accessibility portions of these laws.

45.5.1.3 The Secretary of State may use and rely upon the testing of a voting system performed by a VSTL or by another state upon satisfaction of the following conditions:

(a) The Secretary of State has complete access to any documentation, data, reports or similar information upon which the VSTL or another state relied in performing its tests and will make such
information available to the public subject to any redaction required by law; and

(b) The Secretary of State makes written findings and certifies that he or she has reviewed such information and determines that the tests were conducted in accordance with appropriate engineering standards in use when the tests were conducted and the extent to which the tests satisfy the requirements of sections 1-5-615 and 1-5-616, C.R.S., and all rules promulgated under those sections.

[CURRENT RULE 45.5.1.3 IS MENDED AND MOVED TO RULE 45.5.12(A).]

[Rule 45.5.2.4.3 is amended and moved to New Rule 45.5.3(a). (Modifications to Rule 45.5.2.4.3 are shown below).]

45.5.2 State Standards

45.5.3 Independent Analysis

45.5.2.4.3(A) Prior to completion of functional testing, all voting system providers submitting a voting system shall have completed an independent analysis of the system, which shall include:

(a) The independent analysis shall include:

(i)(1) An application penetration test conducted to analyze the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The test shall involve active exploitation of security vulnerabilities of the voting system, whether or not the vulnerabilities can be mitigated through compensating controls.

(ii)(2) A source code evaluation conducted pursuant to the requirements identified in Rule 45.5.2.6.1(f), requiring compliance with the 2002 voting system standards in accordance with software design and coding standards of the 2002 Voting System Standard or the most current version of the Voluntary Voting System Guidelines that has been approved after January 1, 2008.

(b)(3) A complete report detailing all findings and recommended compensating controls for vulnerabilities and deficiencies identified.

(e)(4) The vendor voting system provider shall use an EAC approved VSTL, at least one of the following to perform the independent analysis, or submit the results of testing conducted in
another state, or some combination of such VSTL and state testing that meets the requirements of this rule:

(i) (A) AN EAC APPROVED VSTL;

(ii) (B) TESTING CONDUCTED IN ANOTHER STATE;

(iii) (C) SOME COMBINATION OF SUCH VSTL AND STATE TESTING THAT MEETS THE REQUIREMENTS OF THIS RULE.

(d)(5) The Secretary of State or VSTL shall conduct a quality review of all work under this section. The review may include an examination of the testing records, interviews of the individuals who performed the work, or both. Review of testing records may be conducted at the VSTL, the state in which the testing was conducted, or at the site of any contractor or subcontractor utilized by another state to conduct the testing.

(e)(6) When an analysis performed by another state is used, the Secretary of State has the right to reject any evaluation if not satisfied with the work product and to require additional analysis to meet the requirements of section 1-5-608.5, C.R.S., and this Rule.

[Rule 45.5.2.1 is amended and moved to New Rule 45.5.4. (Modifications to Rule 45.5.2.1 are shown below).]

45.5.2.1-45.5.4 Functional requirements

45.5.2.1.1 (A) Functional requirements shall address any and all detailed operations of the voting system related to the management and controls required to successfully conduct an election on the voting system.

45.5.2.1.2 (B) The voting system shall provide for appropriately authorized users to:

(a) Prepare the system for an election;

(b) (1) Setup and prepare ballots for an election;

(c) (2) Lock and unlock system to prevent or allow changes to ballot design;

(d) (3) Conduct hardware and diagnostic testing as required herein;

(e) (4) Conduct logic and accuracy testing as required herein;

(f) (5) Conduct an election and meet additional requirements as identified in this section—RULE 45 for procedures for voting, auditing
information, inventory control, counting ballots, opening and closing polls, recounts, reporting and accumulating results— as required herein;

(g) (6) Conduct the post election audit as required herein; and

(h) (7) Preserve the system for future election use.

45.5.2.1.3 (c) The voting system shall integrate Election Day-ELECTION DAY voting results with mail-in, early voting and provisional ballot results.

45.5.2.1.4 — The voting system shall be able to count all of an elector’s votes on a provisional ballot or only federal and statewide offices and statewide ballot issues and questions, as provided under section 1-8.5-108(2), C.R.S.

45.5.2.1.5 — The voting system shall provide for the tabulation of votes cast in split precincts where all voters residing in one precinct are not voting the same ballot style.

45.5.2.1.6 (d) The voting system shall provide for the tabulation of votes cast in combined precincts at remote sites, where more than one precinct is voting at the same location, on either the same ballot style or ON a different ballot style.

45.5.2.1.7 (e) The voting system shall provide authorized users with the capability to produce electronic files including election results in either ASCII (both comma-delimited and fixed-width) or web-based format that shall contain (a) all data or (b) any user selected data elements from the database. The software shall provide authorized users with the ability to generate these files on an “on-demand” basis. After creating such files, the authorized users shall, at their discretion, have the capability to copy the files to diskette, tape, CD-ROM or to transmit the files to another information system OTHER MEDIA TYPE.

(a)(1) Exports necessary for the Secretary of State shall conform to a format agreed upon by the Secretary of State and the voting system provider. If the voting system provider and the Secretary of State have not previously agreed upon a format, the voting system provider shall provide the Secretary of State with specifications for all available export file formats. As part of the certification test, the voting system provider will demonstrate that preliminary and canvassing level election result data, using one or more of the provided formats, can be imported to a commercially available data management program such as a spreadsheet, database, or report generator which can accept that format and which is used and selected by the Secretary of State’s office. Using the imported data, the Secretary of State’s test team shall confirm that the
election results data may be consolidated with results from one or more additional election jurisdictions, searched, selected, sorted, generate totals from selected subsets of the data, and formatted for reporting.

(b) Export files shall be generated so that election results can be communicated to the Secretary of State on election night both during the accumulation of results and after all results have been accumulated.

[Current Rule 45.2.1.7(b) is amended and moved to Rule 11]

(2) The voting system provider shall demonstrate that preliminary and canvassing level election result data can be imported to a commercially available data management program such as a spreadsheet, database, or report generator.

45.5.2.1.8 (f) The voting system shall include hardware and software to enable the closing of the remote voting location and disabling the acceptance of ballots on all vote tabulation devices to allow for the following:

(a) (1) Machine generated paper record PRINTOUT of the time the voting system was closed.

(b) (2) Readings PRINTOUT of the public counter and protective counter shall become a part of the paper audit record upon disabling the voting system to prevent further voting.

(c) (3) Ability to print an abstract of the count of votes A REPORT which shall contain:

(i) (A) Names of the offices;
(ii) (B) Names of the candidates and party, when applicable;
(iii) (C) A tabulation of votes from ballots of different political parties at the same voting location in a primary election;
(iv) (D) Ballot titles;
(v) (E) Submission clauses of all initiated, referred or other ballot issues or questions; and
(vi) (F) The number of votes counted for or against each candidate or ballot issue.
(d) Abstract shall include an election judge’s certificate and statement that contains:

(i) (G) Date of election (day, month and year);

(ii) (H) Precinct Number (ten digit format);

(iii) (I) County or Jurisdiction Name;

(iv) (J) State of Colorado Area for “STATE OF COLORADO”;

(v) (K) Count of votes as indicated in this section for each contest; and

(vi) (L) An election judge’s certificate with an area for judges’ signatures with the words similar to: “Certified by us”, and “Election Judges”. Space should allow for a minimum of two signatures.

(e) (4) Votes counted by a summary of the voting location and by individual precincts.

(4) (5) Ability to produce multiple copies of the unofficial results at the close of the election.

(g) Ability to accommodate a two page ballot (races on four faces) is required.

[Current Rule 45.5.2.1.8(g) is amended and moved to new Rule 45.5.6(c).]

45.5.2.1.9 Voters voting on a DRE shall be able to navigate through the screens without the use of page scrolling. Features such as next or previous page options shall be used.

45.5.2.1.10 (G) The voting system shall ensure that an election setup may not be changed once ballots are printed and/or election media devices are downloaded for votes to be conducted without proper authorization and acknowledgement by the application administrative account. The application and database audit transaction logs shall accurately reflect the name of the system operator making the change(s), the date and time of the change(s), and the “old” and “new” values of the change(s).

45.5.2.1.11 The voting system shall ensure that all tabulated results will be accurately captured, interpreted, and reported to the level of accuracy required in the 2002 Voting System Standards.
45.5.2.3.13 (H) All DRE or BMD voting devices shall use touch screen technology or other technology providing visual ballot display and selection.

45.5.2.3.14 (I) All electronic voting devices supplied by the voting system provider AND USED AT VOTER SERVICE AND POLLING CENTERS shall have the capability to continue ALL NORMAL VOTING operations and provide continuous device availability during a 2-HOUR period of electrical outage without any loss of election data.

45.5.2.3.16 (J) The voting system shall provide capabilities to protect the confidentiality of voters’ ballot choices.

(a) (1) All optical scan devices, associated ballot boxes and V-VPAT storage devices shall provide physical locks and procedures to prevent disclosure of voters’ confidential ballot choices during and after the vote casting operation.

(b) (2) All DRE devices shall provide randomization of all voter choices and stored electronic ballot information, regardless of format, to prevent disclosure of voters’ confidential ballot choices during and after storage of the voters’ ballot selections.

45.5.2.2 ______ Performance Level

45.5.2.2.1 ______ Performance Level shall refer to any operation related to the speed and efficiency required from the voting system to accomplish the successful conduct of an election on the voting system.

45.5.2.2.2 ______ The voting system shall meet the requirements for casting ballots as detailed in the vendor documentation required for certification.

45.5.2.2.3 ______ The voting system provider shall publish and specify processing standards for each component of the voting system as part of the documentation required for certification.

[Current Rule 45.5.2.2.3 is amended and moved to new Rule 45.5.12(l)]

45.5.2.2.4 ______ For the purpose of evaluating software, the voting system provider shall be required to provide detailed information as to the type of hardware required to execute the software.
[Current Rule 45.5.2.2.4 is amended and moved to new Rule 45.5.12(m)]

45.5.2.2.5 At no time shall third party hardware or software have a
negative effect on performance levels of the voting system
application, unless, through documentation, a voting system
provider specifically details the specific hardware or software, the
performance effect and a workaround for the end user to overcome
the issue.

45.5.2.3-45.5.5 Physical and Design Characteristics

45.5.2.3.1 (A) Physical and design characteristics shall address any and all
external or internal construction of the physical environment of the voting
system or the internal workings of the software necessary for the voting
system to function. The voting system shall substantially comply with
these requirements to be considered successful in the conduct of an
election on the voting system.

45.5.2.3.2 The voting system shall meet the following environmental controls
allowing for storage and operation in the following physical ranges:

(a) Operating Temperature — Maximum 95 Degrees Fahrenheit;
Minimum 50 Degrees Fahrenheit, with maximum humidity of
90%, normal or minimum operating humidity of 15%.

(b) Non-Operating Temperature — Maximum 140 Degrees Fahrenheit;
Minimum minus 4 Degrees Fahrenheit. Non operating humidity
ranges from 5% to 90% for various intervals throughout the day.

The documentation supplied by the voting system provider shall include a
statement of all requirements and restrictions regarding environmental
protection, electrical service, telecommunications service and any other
facility or resource required for the installation, operation and storage of
the voting system.

[Part of current Rule 45.5.2.3.2 is relocated to new Rule 45.5.12(n)]

45.5.2.3.17 (B) The voting system provider shall submit drawings, photographs
and any related brochures or documents to assist with the evaluation of the
physical design of the use of the voting system.

45.5.6 BALLOT DEFINITION SUBSYSTEM

45.5.2.3.3 (A) The ballot definition subsystem of the voting system application
consists of hardware and software required to accomplish the functions
outlined in this Rule 45.5.2.3-45.5.6. System databases contained in the
ballot definition subsystem may be constructed individually or they may
be integrated into one database. These databases are treated as separate
databases to identify the necessary types of data to be handled and to specify, where appropriate, those attributes that can be measured or assessed for determining compliance with the requirements of this standard.

45.5.2.3.4—The ballot definition subsystem shall be capable of formatting ballot styles in English and any alternate languages as are necessary to comply with The “Voting Rights Act of 1965” 42 U.S.C. § 1973c et seq. (1965).

45.5.2.3.5—The voting system application shall allow the operator to generate and maintain an administrative database containing the definitions and descriptions of political subdivisions and offices within the jurisdiction.

45.5.2.3.6—The ballot definition subsystem shall provide for the definition of political and administrative subdivisions where the list of candidates or contests may vary within the remote site and for the activation or exclusion of any portion of the ballot upon which the entitlement of a voter to vote may vary by reason of place of residence or other such administrative or geographical criteria. This database shall be used by the system with the administrative database to format ballots or edit formatted ballots within the jurisdiction.

45.5.2.3.7—For each election, the subsystem shall allow the user to generate and maintain a candidate and contest database and provide for the production and/or definition of properly formatted ballots and software.

45.5.2.3.8—(b) The ballot definition subsystem shall be capable of handling at least 500 200 potentially active voting positions, arranged to identify party affiliations in a primary election, offices with their associated labels and instructions, candidate names with their associated labels and instructions and ballot issues or questions with their associated text and instructions.

45.5.2.3.9—The ballot display may consist of a matrix of rows or columns assigned to political parties or non-partisan candidates and columns or rows assigned to offices and contests. The display may consist of a contiguous matrix of the entire ballot or it may be segmented to present portions of the ballot in succession.

45.5.2.3.10—(C) Ability to—The voting system must accommodate a single page ballots (races on one face or both faces) and two page ballot paper ballots (races on three or four faces) is required.

45.5.2.3.10—(D) The voting system application shall—Balloon definition subsystem must:

(1) provide a facility for the definition of the ballot, including the definition of the number of allowable choices for each office
and contest and for special voting options such as write-in candidates. It shall provide for all voting options and specifications as provided for in Articles 5 and 7, Title 1, C.R.S.;

(2) The system shall generate generate all required masters and distributed copies of the voting program in conformance with the definition of the ballot for each voting device and remote site election management software. The distributed copies, resident or installed, in each voting device shall include all software modules required to monitor system status and generate machine level audit reports, accommodate device control functions performed by remote location officials and maintenance personnel and register and accumulate votes.

45.5.7 Trusted Build

45.5.2.3.11—The trusted build of the voting system software, installation programs and third party software used to install or to be installed on voting system devices shall be distributed on a write-once media.

45.5.2.3.12—The voting system shall allow the system administrative account to verify that the software installed is the certified software by comparing it to the trusted build or other reference information.

45.5.2.3.13—All DRE voting devices shall use touch screen technology or other technology providing visual ballot display and selection. The voting system provider shall provide documentation concerning the use of touch screen or other display and selection technology including, but not limited to:

(a) Technical documentation describing the nature and sensitivity of the tactile device (if the system uses touch screen technology);

(b) Technical documentation describing the nature and sensitivity of any other technology used to display and select offices, candidates or issues;

[Current Rule 45.5.2.3.13 is amended and moved to new Rule 45.5.4(h). Current Rule 45.5.2.3.13(a)-(b) are amended and moved to new Rule 45.5.12(c).]

(c) Any mean time between failure (MTBF) data collected on the vote recording devices; and

(d) Any available data on problems caused for persons who experience epileptic seizures due to the DRE voting device's screen refresh rate.
45.5.2.3.14 All electronic voting devices supplied by the voting system provider shall have the capability to continue operations and provide continuous device availability during a period of electrical outage without any loss of election data.

(a) For optical scan devices, this capability shall include, at a minimum, for a period of not less than two hours the ability to:

(i) Continue to scan or image voters’ ballots;

(ii) Accurately tabulate voters’ choices from the ballots;

(iii) Accurately store voters’ ballot choices; and

(iv) Transmit required results files accurately if power failure occurs during transmittal of results.

(b) For DRE devices, this capability shall include, at a minimum, for a period of not less than two hours the ability to:

(i) Continue to present ballots accurately to voters;

(ii) Accept voters’ choices accurately on the devices;

(iii) Tabulate voters’ choices accurately;

(iv) Store voters’ choices accurately in all storage locations on the device; and

(v) Transmit required results files accurately if power failure is experienced during transmittal of results.

(c) For V-VPAT devices connected to DREs, this capability shall include, at a minimum, for a period of not less than two hours the ability to:

(i) Continue to print voters’ choices on the DRE accurately and in a manner that is identical to the manner of the printers’ operations during a period of normal electrical operations; and
(ii) Continue to store the printed ballots in a secure manner that is identical to the manner of the printers’ operations during a period of normal electrical operations.

(d) The voting system provider shall deliver to the Secretary of State documentation detailing estimated time of battery operation for each type of optical scanner, ballot imager, DRE and V-VPAT they provide, assuming continuous use of the devices by voters during an interruption of normal electrical power.

(e) The voting system provider shall deliver to the Secretary of State documentation specifying the steps and times required for charging batteries for each type of optical scanner, ballot imager, DRE and V-VPAT they provide.

[Current 45.5.2.3.14 (d) and (e) are amended and moved to new rule 45.5.12(e) and (p) and (q).]

45.5.2.3.15 The voting system provider’s software application shall be able to recover operations after a power outage or other abnormal shutdown of the system on which that application and database are operating without loss of more than the current transaction data record on which the administrative account or authorized operator account is currently working.

[Current 45.5.2.3.15 is amended and moved to new Rule 45.5.4(j)]

45.5.2.3.16 The voting system shall provide capabilities to protect the confidentiality of voters’ ballot choices.

(a) All optical scan devices, associated ballot boxes and V-VPAT storage devices shall provide physical locks and procedures to prevent disclosure of voters’ confidential ballot choices during and after the vote casting operation.

(b) All DRE devices shall provide randomization of all voter choices and stored electronic ballot information, regardless of format, to prevent disclosure of voters’ confidential ballot choices during and after storage of the voters’ ballot selections.

[Current 45.5.2.3.16 is amended and moved to new Rule 45.5.4(j)]

45.5.2.3.17 The voting system provider shall submit drawings, photographs and any related brochures or documents to assist with
the evaluation of the physical design of the use of the voting system.

[Current 45.5.2.3.17 is moved to new Rule 45.5.5(b).]

45.5.2.4 Documentation Requirements

45.5.2.4.1 In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents:

(a) Standard Issue Users/Operator Manual;

(b) System Administrator’s/Application Administration Manual;

(c) Training Manual and related materials;

(d) Systems Programming and Diagnostics Manuals; and

(e) A list of minimum services needed for the successful, secure and hardened operation of all components of voting system.

[Current Rule 45.5.2.4 amended and moved to new rule 45.5.12.]

45.5.2.4.2 For the review of VSTL or other state testing in Rule 45.5.1.3 copies of all VSTL or state qualification reports, test logs and technical data packages shall be provided to the Secretary of State:

(a) The voting system provider shall execute and submit any necessary releases for the applicable VSTL, state and/or EAC to discuss any and all procedures and findings relevant to the voting system submitted for certification with the Secretary of State and allow the review by the Secretary of State of any documentation, data, reports or similar information upon which the VSTL or other state relied in performing its testing. The voting system provider shall provide a copy of the same to the Secretary of State.

(b) The voting system provider, the VSTL, the state and/or the EAC will identify to the Secretary of State any specific sections of documents for which they assert a legal requirement for redaction.
45.5.2.4.3 — Prior to completion of functional testing, all voting system providers submitting a voting system shall have completed an independent analysis of the system.

(a) — The independent analysis shall include:

(i) — An application penetration test conducted to analyze the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The test shall involve active exploitation of security vulnerabilities of the voting system, whether or not the vulnerabilities can be mitigated through compensating controls.

(ii) — A source code evaluation conducted pursuant to the requirements identified in Rule 45.5.2.6.1(f), requiring compliance with the 2002 voting system standards.

(b) — A complete report detailing all findings and recommended compensating controls for vulnerabilities and deficiencies identified.

(c) — The vendor shall use an EAC approved VSTL to perform the independent analysis, or submit the results of testing conducted in another state, or some combination of such VSTL and state testing that meets the requirements of this rule.

(d) — The Secretary of State shall conduct a quality review of all work under this section. The review may include an examination of the testing records, interviews of the individuals who performed the work, or both. Review of testing records may be conducted at the VSTL, the state in which the testing was conducted, or at the site of any contractor or subcontractor utilized by another state to conduct the testing.

(e) — When an analysis performed by another state is used, the Secretary of State has the right to reject any evaluation if not satisfied with the work product and to require additional analysis to meet the requirements of section 1-5-608.5, C.R.S., and this Rule.
45.5.2.4.4 — Documentation submitted to the Secretary of State shall be reviewed to determine the extent to which the voting system has been tested to federal standards.

45.5.2.4.5 — Documentation shall include the financial statements set forth in Rule 45.13, which shall be for the prior fiscal year, and any quarterly financial statements for the period following the prior fiscal year and preceding the date of application for certification.

45.5.2.4.6 — Failure by the voting system provider to provide any documentation with their application for certification will delay processing the application until the documentation is provided.

45.5.2.5 — Audit capacity

45.5.2.5.1 — The voting system shall be capable of producing electronic and printed audit logs of system operation and system operators’ actions which shall be substantially compliant to allow operations and input commands to be audited.

45.5.2.5.2 — The voting system shall include detailed documentation as to the level, location and programming of audit trail information throughout the system. The audit information shall apply to:

(a) — Operating Systems (workstation, server and/or DRE);

(b) — Election Programming Software;

(c) — Election Tabulation Devices—optical scan and DRE; and

(d) — Election Reporting Subsystem.

45.5.2.5.3(A) — The voting system shall track and maintain audit information of the following voting system application—ELECTION MANAGEMENT SYSTEM events:

(a)(1) — Log on and log off activity;

(b)(2) — Application start and stop;
(e)(3) Printing activity, where applicable;

(d)(4) Election events – setup, set for election, unset for election, open polls, close polls, end election, upload devices, download devices, create ballots, create precincts, create districts, create poll places (or Vote Centers), VOTER SERVICE AND POLLING CENTERS, initialize devices, backup devices and voting activity; and

(e)(5) Hardware events – add hardware, remove hardware, initialize hardware and change hardware properties.

45.5.2.5.4(b) All tabulation devices shall display the unit serial number(s) both physically and within any applicable software, logs or reports.

45.5.2.5.5(c) Vote tabulation devices shall allow for an alternate method of transfer of audit records if the device or a memory storage device is damaged or destroyed.

45.5.2.5.6(d) All transaction audit records of the voting system application ELECTION MANAGEMENT SYSTEM database shall be maintained in a file outside of or separate from the database IN A READ-ONLY FORMAT, which is not accessible by user/operator accounts.

45.5.2.6 45.5.9 Security Requirements REQUIREMENTS

45.5.2.6.1(A) All voting systems submitted for certification shall meet the following minimum system security requirements:

(a)(1) The voting system shall MEET THE FOLLOWING REQUIREMENTS TO accommodate a general system of access by least privilege and role based ROLE-BASED access control. The following requirements shall apply:

(i)(A) The operating OPERATING system administrative account ACCOUNTS shall not have access to read or write data to the database and shall not have the ability or knowledge of the database administrator password;

(ii) The operating system administrative account shall not be required to use any function of the voting system during normal operations;

(iii)(B) A unique OPERATING system user/operator account ACCOUNTS shall be ABLE TO BE created for operating system use that is ARE restricted from the following aspects of the operating system:

a.(I) No access to system root directory;
b.- (II) No access to operating system specific folders;

e.- (III) No access to install or remove programs; and

d.- (IV) No access to modify other user accounts on the system.

(iv) (C) A unique application administrative account shall be created which has full access and rights to the application and database;

(v) (D) A unique application user/operator account shall be created with limited rights specifically designed to perform functional operation within the scope of the application. This user/operator shall be restricted in the creation or modification of any user/operator accounts; and

(vi) The voting system provider shall not have an administrative account or administrative account access.

[Current Rule 45.5.2.6.1(a)(vi) mMoved to Rule 43]

(b) (2) The voting system shall meet the following requirements for network security:

(i) (A) All components of the voting system shall have the ability to operate on a closed network dedicated to the voting system;

(ii) (B) All components of the voting system shall include the limited use of non-routable IP address configurations for any device connected to the closed network. For the purposes of this requirement, non-routable IP addresses are those defined in the RFC 1918 Address base; and

(iii) (C) The voting system shall be tested to contain provisions for updating security patches, software and/or service packs without access to the open network.

(e) (3) All voting systems submitted for certification that use databases shall meet the following requirements for database security:

(i) All voting systems submitted for certification shall have databases hardened to specifications developed by the voting system provider. Documentation included with the application shall provide a detailed procedure for
The voting system shall meet the following requirements for operating system security:

(i)(A) All voting systems submitted for certification shall have all operating systems hardened to specifications developed by the voting system provider. Documentation included with the application shall provide a detailed procedure for hardening and the procedure used to harden the system. Any government or industry guidelines adopted in whole, or in part, are to be identified in the documentation.

(ii) The voting system provider shall submit documentation containing a list of minimum services and executables required to run the voting system application.

[Current Rule 45.5.2.6.1(d)(ii) is amended and moved to new Rule 45.5.12 (r)]

(iii)(B) The voting system provider shall configure the voting system operating system of the workstation and/or server used for the election management software to the following requirements:

a. (I) The ability for the system to take an action upon inserting a removable media (Auto run) shall be disabled; and

b. (II) The operating system shall only boot from the drive or device identified as the primary drive. The voting system shall not boot from any alternative device.

(iv)(C) The voting system provider shall use a virus protection/prevention application on the election management server(s)/workstations which shall be capable of manual updates without the use of DIRECT CONNECTION TO the internet.

(e)(5) The voting system shall meet the following requirements for password security:

(i)(D) All passwords shall be stored and used in a non-reversible format;
(iii)-(E) Passwords to THE database shall not be stored in THE database;

(iii)-(F) Password to THE database shall be owned and only known by the application;

(iv) (G) The application’s database management system shall require separate passwords for the administrative account and each operator account with access to the application;

(v) (H) The system shall be designed in such a way to ensure that the use of the administrative account password shall IS not be required for normal operating functions at any remote location;

(vi)-(I) The system shall be designed in such a way to facilitate the changing of passwords for each election cycle;

(vii) (J) The use of blank or empty passwords shall not be permitted at any time with the exception of a limited one-time use startup password which requires a new password to be assigned before the system can be used; and

(viii)-(K) All voting systems submitted for certification shall have all components of THE voting system capable of supporting passwords of a minimum of eight characters, which AND shall be capable of including numeric, alpha and special characters in upper case or lower case used in any combination.

(f) All voting system software submitted for certification shall be in compliance with the Software Design and Coding Standards of the Voting System Standards adopted in Rule 37.3.

(g)-(6) All modules of the system shall meet the following 2002 VOTING SYSTEM STANDARDS requirements for installation of software, including hardware with embedded firmware:

(i) If software is resident in the system as firmware, the voting system provider shall provide documentation that describes how devices may be retested to validate each ROM prior to the start of elections operations.

(ii) No software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction shall provide a secure physical and
procedural environment for the storage, handling, preparation and transportation of the system hardware.

(iii) The voting system bootstrap, monitor and device controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program and its associated exception handlers.

(iv) The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

(v) After initiation of Election Day testing under Rule 11.5.3, no source code, compilers or assemblers shall be resident or accessible.

(vi) (A) Where the system includes a feature to interpret and control execution using data from a script, code tokens, or other form of control data file separate from the source code, the human-readable source information shall be made available as part of the A source code review and the data files used shall be defined and controlled as part of the Trusted Build as if it were part of the executable code.

(vii) (B) Security features and procedures shall be defined and implemented to prevent any changes of interpreted data files after the initial election testing of the final election definition and only allow authorized replacement of the data files with tested and approved files from the Trusted Build. TRUSTED BUILD SHALL BE BY authorized personnel before the election definition is finalized for an election.

(viii) (C) The introduction of interpreted data during execution shall not be permitted unless defined as a predefined set of commands or actions subject to security review and the interpretation function provides security edits on input to prevent the introduction of other commands or the modification or replacement of existing code.

(ix) Independent analysis will test for the following conditions and report on absence or presence of the following input validations in accordance with Rule 45.5.2.4.3:
a. Path manipulation;

b. Cross-Site Scripting;

c. Resource Injection;

d. OS Command Injection (also called “Shell Injection”); and

e. SQL Injection.

(x) Independent analysis will test for the following conditions and report on their absence or presence of the following range errors in accordance with Rule 45.5.2.4.3:

a. Stack Overflow;

b. Heap Overflow;

c. Format string vulnerability; and

d. Improper Null Termination.

(xi) Independent analysis will test for the following conditions and report on their absence or presence of the following Application Programming Interface (API) abuses in accordance with Rule 45.5.2.4.3:

a. Heap Inspection; and

b. String Management/Manipulation.

(xii) Independent analysis will test for the following conditions and report on the absence or presence of the following time and state conditions in accordance with Rule 45.5.2.4.3:

a. Time-of-check/Time-of-use race condition; and

b. Unchecked Error Condition.

(xiii) Independent analysis will test for the following conditions and report on the absence or presence of the following code quality conditions accordance with Rule 45.5.2.4.3:

a. Memory Leaks;

b. Unrestricted Critical Resource Lock;

c. Double Free;
d. Use After Free;  
  
e. Uninitialized variable;  
  
f. Unintentional pointer scaling;  
  
g. Improper pointer subtraction; and  
  
h. Null Dereference.  

(xiv) Independent analysis will test for the following conditions and report on the absence or presence of the following encapsulation conditions in accordance with Rule 45.5.2.4.3:  

a. Private Array-Typed Field Returned from a Public Method;  
  
b. Public Data Assigned to Private Array-Typed Field;  
  
c. Overflow of static internal buffer; and  
  
d. Leftover Debug Code.  

(xv) (D) The application shall not open database tables for direct editing.  

(h) All voting systems submitted for certification shall meet the following minimum requirements for removable storage media with data controls:  

(i) All voting data stored that includes vote records, ballot images, tally data and cast votes—VOTE RECORDS shall be authenticated and validated.  
  
(ii) All non-voting data stored shall be authenticated, encrypted, and validated.  
  
(iii) All removable media, upon insertion of media or media device on server and/or workstations hosting the elections management software, shall automatically be scanned by antivirus software.  

45.5.2.6.2 The voting system provider shall provide documentation detailing voting system security in the areas listed below. The system shall contain documented configurations, properties and procedures to prevent, detect and log changes to system capabilities for:  

(a) Defining ballot formats:
(b) Casting and recording votes;

c) Calculating vote totals consistent with defined ballot formats;

d) Reporting vote totals;

e) Altering of voting system audit records;

f) Changing or preventing the recording of a vote;

g) Introducing data for a vote not cast by a registered voter;

h) Changing calculated vote totals;

i) Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and

j) Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

[Current Rule 45.5.2.6.2 amended and moved to new Rule 45.5.12(i)]

45.5.2.6.3 The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing:

(a) Software access controls;

(b) Hardware access controls;

(c) Data communications;

(d) Effective password management;

(e) Protection abilities of a particular operating system;

(f) General characteristics of supervisory access privileges;

(g) Segregation of duties; and

(h) Any additional relevant characteristics.

45.5.2.6.4 The voting system shall include detailed documentation regarding the security measures it has in place for all systems, applicable software, devices that act as connectors (upload, download, and other programming devices) and any security measures the voting system provider recommends to the jurisdictions that purchase the voting system.
45.5.2.7.1 (A) Telecommunications includes all components of the system that transmit data outside of the closed network as defined in this Rule 45.

45.5.2.7.2 (B) All electronic transmissions from a voting system shall meet the following minimum standards—2002 Voting System Standards.

(a)-(C) Modems from remote devices shall be programmed to be “dial only” and cannot be programmed to NOT receive a call;

(b) Use an encryption standard currently documented and validated for use by an agency of the United States Federal Government; and

(c) Provide a means to detect the presence of an intrusive process, such as an Intrusion Detection System.

45.5.2.7.3 (D) Any modem in any component failing to meet these criteria—The requirements of this Rule shall not be used by any voting system.

45.5.2.7.4 (E) All wireless components in voting systems shall be disabled with the exception of line—Line of sight infrared technology shall only be used in a closed environment where the transmission and reception is shielded from external infrared signals and can only accept infrared signals generated from within the system.

45.5.2.7.5 (F) All systems that transmit data over public telecommunications networks shall maintain a clear audit trail that can be provided to the Secretary of State when election results are transmitted by telephone, microwave or other type of electronic communication.

45.5.2.7.6 Systems designed for transmission of voter information over public networks shall meet security standards that address the security risks attendant with the casting of ballots at remote sites controlled by election officials using the voting system configured and installed by election officials and/or their voting system provider or contractor, and using in-person authentication of individual voters.

45.5.2.7.7 Any voting system provider of systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:

(a) All activities mandatory to ensure effective system security to be performed in setting up the system for operation, including testing security before an election.
(b) All activities that should be prohibited during system setup and during the time frame for voting operations, including the hours when polls are open and when polls are closed.

45.5.2.7.8 (g) In any situation in which the voting system provider’s system transmits voting systems that transmit data through any telecommunications medium, the system shall be able to recover, either automatically or with manual intervention, from incomplete or failed transmission sessions and resume transmissions automatically when telecommunications are re-established.

(a)(1) Recovery of transmissions shall include notations of the interrupted transmission session and the resumed transmission session in the system and application transaction logs.

(b)(2) Failure and recovery of transmissions shall not cause any error in data transmitted from the polling place—voter service and polling centers to the central election site during a recovered transmission session.

45.5.2.7.9 Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software. Documentation shall identify the name, voting system provider and version used for each such component.

45.5.2.7.10 Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

(a) Monitor threats, such as through the review of assessments, advisories and alerts for COTS components;

(b) Evaluate the threats and, if any, proposed responses;

(c) Develop responsive updates to the system and/or corrective procedures; and

(d) As part of the certification requirements of the proposed system, provide assistance to customers, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the Secretary of State.
45.5.2.8 Repealed.

45.5.2.9-45.5.11 Voter-Verifiable Paper Record Requirements (VVPAT) Voter-Verifiable Paper Record Requirements

45.5.2.9.1 V-VPAT shall refer to a Voter-verified paper record as defined in section 1-1-104(50.6)(a), C.R.S.

[Current Rule 45.5.2.9.1 is amended and moved to New Rule 45.1.22.]

45.5.2.9.2 (a) Existing systems that are retrofitted to comply with this law SECTION 1-5-802(1), C.R.S., shall be examined for certification by the Secretary of State. Any retrofitted voting system shall comply with the process and application for certification as identified by this Rule 45.

45.5.2.9.3 (b) The V-VPAT—VVPAT shall consist of the following minimum components:

(a) (1) The voting device shall contain a paper audit trail writer or printer that shall be attached, built into or used in conjunction with the DRE; the printer shall duplicate a voter’s selections from the DRE onto a paper record;

(b) (2) The unit or device shall have a paper record display unit or area that shall allow a voter to view his or her paper record; AND

(c) (3) The V-VPAT unit shall contain a paper record storage unit that shall store cast and spoiled paper record copies securely; and

(d) These devices may be integrated as appropriate to their operation.

45.5.2.9.4 V-VPAT devices shall allow voters to verify his or her selections on a paper record prior to casting ballots. The voter shall either accept or reject the choices represented on the paper record. Both the electronic record and the paper record shall be stored and retained when the ballot is cast.

45.5.2.9.5 The V-VPAT printer connection may be any standard, publicly documented printer port (or the equivalent) using a standard communication protocol.

(c) The VVPAT shall meet the following functional requirements:

45.5.2.9.6 (1) The printer may only communicate with any device other than the voting device to which it is connected;
45.5.2.9.7 (2) The printer shall only be able to function as a printer, and not perform any other non-printer related services.

45.5.2.9.8 (3) Every electronic voting record shall have a corresponding paper record. PRODUCE A PAPER RECORD FOR EVERY CORRESPONDING ELECTRONIC VOTING RECORD;

45.5.2.9.9 (4) The paper record shall be considered an official record of the election available for recounts, and shall be sturdy, clean, and of sufficient durability to be used for this purpose.

45.5.2.9.16 (4) The V-VPAT unit shall provide a “low supply” warning to the election judge to add paper, ink, toner, ribbon or other like supplies. In the event that an election judge is required to change supplies during the process of voting, the voter shall be allowed to reprint and review the paper audit trail RECORD without having to re-mark his or her ballot. The device shall prevent the election judge from seeing any voters’ ballots A VOTER’S BALLOT.

45.5.2.9.17 (5) All voting systems submitted for certification shall stop the V-VPAT printer of all forward operations of the DRE STOP ALL OPERATIONS if the printer is not working due to paper jams, out of other consumables or any other issue which may cause the correct readable printing of information on the V-VPAT record as designed.

45.5.2.9.20 (6) The V-VPAT shall allow a voter to spoil his or her paper record no more than two times. Upon spoiling, the voter shall be able to modify and verify selections on the DRE without having to reselect all of his or her choices.

45.5.2.9.21 (7) Before the voter causes a third and final record to be printed, the voter shall be presented with a warning notice that the selections made on screen shall be final and the voter shall see and verify a printout of his or her vote, but shall not be given additional opportunities to change their vote.

45.5.2.9.22 (8) When V-VPAT components are integrated into a previously certified voting system, the new configuration of the voting system must comply with existing state testing and auditing requirements.

45.5.2.9.23 (9) The V-VPAT component should print a barcode with each record that contains the human readable contents of the paper record and digital signature information. The voting system provider shall include documentation of the barcode type, protocol,
and/or description of barcode and the method of reading the barcode as applicable to the voting system.

45.5.2.9.25(10) If used for provisional ballots, the V-VPAT system VVPAT shall be able to mark paper records as a provisional ballot through the use of human readable text and optionally printing barcode and/or serial number information which shall provide for mapping the record back to the electronic record and the provisional voter for processing after verification in accordance with Article 8.5 of Title 1, C.R.S.

(D) THE VVPAT SHALL MEET THE FOLLOWING DESIGN REQUIREMENTS:

45.5.2.9.10(1) The V-VPAT device shall be designed to allow every voter to review and accept or reject his/her paper record in as private and independent manner as possible for both disabled and non-disabled voters REGARDLESS OF WHETHER THE VOTER HAS DISABILITY.

45.5.2.9.11(2) The V-VPAT system shall be designed in conjunction with state law to ensure the secrecy of votes so that it is not possible to determine which voter cast which paper record.

45.5.2.9.12(2) The V-VPAT printer shall print PRINT at a font size no less than ten-point 14-POINT SANS-SERIF ARIAL for ease of readability. Any protective covering intended to be transparent shall be in such condition that it can be made transparent by ordinary cleaning of its exposed surface.

45.5.2.9.13(3) The V-VPAT system shall be designed to allow each voter to verify his or her vote on a paper record in the same language THAT they voted in on the DRE.

45.5.2.9.14(4) The V-VPAT system shall be designed to prevent tampering with unique keys and/or seals for the compartment that stores the paper record as well as meet the security requirements of this rule. Additional security measures may be in place on the printer to prevent tampering with the device.

45.5.2.9.15(5) The V-VPAT system shall be capable of printing and storing PRINT AND STORE paper record copies for at least 75 ballots cast without requiring the paper supply source, ink or toner supply, or any other similar consumable supply to be changed, assuming a fully printed double sided 18 inch ballot with a minimum of 20 contests.

45.5.2.9.16(6) The V-VPAT unit shall provide a “low supply” warning to the election judge to add paper, ink, toner,
ribbon or other like supplies. In the event that an election judge is required to change supplies during the process of voting, the voter shall be allowed to reprint and review the paper audit trail without having to re-mark his or her ballot, and the device shall prevent the election judge from seeing any voters’ ballots.

[Current Rule 45.5.2.9.16 is amended and moved to New Rule 45.5.11(c)(4).]

45.5.2.9.17—All voting systems submitted for certification shall stop the V-VPAT printer of all forward operations of the DRE if the printer is not working due to paper jams, out of other consumables or any other issue which may cause the correct readable printing of information on the V-VPAT record as designed.

[Current Rule 45.5.2.9.17 amended and moved to New Rule 45.5.11(c)(5).]

45.5.2.9.18—The voting system provider shall provide procedures and documentation for the use of the V-VPAT device.

[Current Rule 45.5.2.9.18 amended and moved to New Rule 45.5.12(k).]

45.5.2.9.19—(6) The printed information on the printed ballot or verification portion of the V-VPAT device PAPER RECORD shall contain at least the following items:

(a)-(A) Name or header information of race, question or issue;

(b)-(B) Voter’s selections for the race information;

(c)-(C) Write-in candidate’s names if selected;

(d)-(D) Undervote or overvote information—this is in addition to the information on the review screen of the DRE;

(e)-(E) Ability to optionally produce a unique serial number (randomized to protect privacy); and

(f)-(F) Identification that the ballot was cancelled or cast.

45.5.2.9.20—The V-VPAT shall allow a voter to spoil his or her paper record no more than two times. Upon spoiling, the voter shall be able to modify and verify selections on the DRE without having to reselect all of his or her choices.
45.5.2.9.20 — Before the voter causes a third and final record to be printed, the voter shall be presented with a warning notice that the selections made on screen shall be final and the voter shall see and verify a printout of his or her vote, but shall not be given additional opportunities to change their vote.

45.5.2.9.21 — When V-VPAT components are integrated into voting systems, the new configuration of the system must comply with existing state testing and auditing requirements.

45.5.2.9.22 — The V-VPAT component should print a barcode with each record that contains the human readable contents of the paper record and digital signature information. The voting system provider shall include documentation of the barcode type, protocol, and/or description of barcode and the method of reading the barcode as applicable to the voting system.

45.5.2.9.23 — The V-VPAT component shall be designed such that a voter shall not be able to leave the voting area with the paper record.

45.5.2.9.24 — If used for provisional ballots, the V-VPAT system shall be able to mark paper records as a provisional ballot through the use of human readable text and optionally printing barcode and/or serial number information which shall provide for mapping the record back to the electronic record and the provisional voter for processing after verification in accordance with Article 8.5 of Title 1, C.R.S.

45.5.2.9.25 — The voting system provider shall provide procedures to the Secretary of State with the application for certification which describe DOCUMENTATION DESCRIBING how to investigate and resolve malfunctions including, but not limited to the following:
misreporting votes, unreadable paper records, paper jams, low ink, misfeeds, preventing the V-VPAT from being a single point of failure, recovering votes in the case of malfunction and power failures.

(A) MISREPORTING VOTES;

(B) UNREADABLE PAPER RECORDS;

(C) PAPER JAMS;

(D) LOW-INK;

(E) MISFEEDS;

(F) LOST VOTES; AND

(G) POWER FAILURES.

45.5.2.4 45.5.12 Documentation Requirements

45.5.1.3 (A) The Secretary of State may use and rely upon the testing of a voting system performed by a VSTL or by another state upon satisfaction of the following conditions:

(a)-(1) The Secretary of State has complete access to any documentation, data, reports or similar information upon which the VSTL or another state relied in performing its tests and will make such information available to the public subject to any redaction required by law; and

(b)-(2) The Secretary of State makes written findings and certifies that he or she has reviewed such information and determines HAS DETERMINED that the tests were conducted in accordance with appropriate engineering standards in use when the tests were conducted, and the extent to which the tests satisfy the requirements of sections 1-5-615 and 1-5-616, C.R.S., and all rules promulgated under those sections.

45.5.2.4.1 (B) In addition to other documentation requirements in this rule, the voting system provider shall provide the following documents:

(a)(1) Standard Issue Users/Operator Manual;
(b)(2) System Administrator’s/Application Administration Manual—ADMINISTRATOR’S/APPLICATION ADMINISTRATION MANUAL;

(e)(3) Training Manual—MANUAL and related materials;

(d)(4) Systems Programming—PROGRAMMING and Diagnostics Manuals—DIAGNOSTICS MANUALS; and

(e)(5) A list of minimum services needed for the successful, secure and hardened operation of all components of THE voting system.

45.4.2.13-(c) The voting system provider shall provide documentation concerning the use of touch screen or other display and selection technology including, but not limited to:

(a)-(1) Technical documentation describing the nature and sensitivity of the tactile device (if the system uses touch screen technology);

(b)-(2) Technical documentation describing the nature and sensitivity of any other technology used to display and select offices, candidates or issues;

45.5.2.4.2-(d) For the review of VSTL or other state testing in Rule 45.5.1.3 45.5.12(∆) copies of all VSTL or state qualification reports, test logs and technical data packages shall be provided to the Secretary of State.

(a)-(1) The voting system provider shall execute and submit any necessary releases for the applicable VSTL, state and/or EAC to discuss any and all procedures and findings relevant to the voting system submitted for certification with the Secretary of State and allow the review by the Secretary of State of any documentation, data, reports or similar information upon which the VSTL or other state relied in performing its testing. The voting system provider shall provide a copy of the same to the Secretary of State.

(b)-(2) The voting system provider, the VSTL, the state and/or the EAC will identify to the Secretary of State any specific sections of documents for which they assert a legal requirement for redaction.

45.5.2.3.14-(d)-(e) The voting system provider shall deliver to the Secretary of State documentation detailing estimated time of battery operation for each type of optical scanner, ballot imager, DRE and V-VPAT they provide,
assuming continuous use of the devices by voters during an interruption of normal electrical power.

45.5.2.3.14(e) The voting system provider shall deliver documentation specifying the steps and times required for charging batteries, AND THE TIME OF BATTERY OPERATION for each type of optical scanner, ballot imager, DRE and VPAT DEVICE they provide, ASSUMING CONTINUOUS USE OF THE DEVICES BY VOTERS DURING AN INTERRUPTION OF NORMAL ELECTRICAL POWER.

45.5.2.4.4 (f) Documentation submitted to the Secretary of State shall be reviewed to determine the extent to which the voting system has been tested to federal standards.

45.5.2.4.6 (g) Failure by the voting system provider to provide any documentation with their application for certification will delay processing the application until the documentation is provided AND MAY BE CAUSE FOR DENIAL OF CERTIFICATION.

45.5.2.5.2 (h) The voting system shall include detailed documentation, WHICH INCLUDES as to the level, location and programming A DESCRIPTION OF THE CONTENT of THE of audit trail information throughout the system. The audit information shall apply to:

(a)(1) Operating Systems (workstation, server, OPTICAL SCANNER, BDM, and/or DRE);

(b)(2) Election Programming Software MANAGEMENT SYSTEM; AND

(c)(3) Election Tabulation Devices – optical scan and DRE; and

(d)——Election Reporting Subsystem.

45.5.2.6.2 (i) The voting system provider shall provide documentation detailing voting system security in the areas listed below. The system DOCUMENTATION shall contain documented configurations, properties and procedures to prevent, detect and log changes to system capabilities for:

(a)(1) Defining ballot formats;

(b)(2) Casting and recording votes;

(c)(3) Calculating vote totals consistent with defined ballot formats;

(d)(4) Reporting vote totals;
(e)(5) Altering of voting system audit records;

(f)(6) Changing or preventing the recording of a vote;

(g)(7) Introducing data for a vote not cast by a registered voter;

(h)(8) Changing calculated vote totals;

(i)(9) Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and

(j)(10) Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

45.5.2.6.4 (j) The voting system provider shall include detailed documentation regarding the security measures it has in place for all systems, applicable software, devices that act as connectors (upload, download, and other programming devices) and any security measures the voting system provider recommends to the jurisdictions that purchase the voting system.

45.5.2.9.18 (k) The voting system provider shall provide procedures and documentation for the use of the V-VPAT device.

45.5.2.2.3 (l) The voting system provider shall publish and specify processing standards for each component of the voting system as part of the documentation required for certification.

45.5.2.2.4 (m) For the purpose of evaluating software, the voting system provider shall be required to provide detailed information as to the type of hardware required to execute the software.

45.5.2.3.2 (n) The documentation supplied by the voting system provider shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service and any other facility or resource required for the installation, operation and storage of the voting system.

45.5.2.3.13(d)(o) Any – The voting system provider shall provide any available data on problems caused for persons who experience epileptic seizures due to the DRE voting device's screen refresh rate.

45.5.2.3.14(d)(p) The voting system provider shall deliver to the Secretary of State documentation detailing estimated time of battery operation for each type of optical scanner, ballot imager, DRE and V-VPAT they provide device submitted for certification, assuming continuous use of the devices by voters during an interruption of normal electrical power.
45.5.2.3.14(e)-(q) The voting system provider shall deliver to the Secretary of State documentation specifying the steps and times required for charging batteries for each type of optical scanner, ballot imager, DRE and V-VPAT they provide. DEVICE SUBMITTED FOR CERTIFICATION.

45.5.2.6.1(d)(ii)-(r) The voting system provider shall submit documentation containing a list of minimum services and executables required to run the voting system application.

45.6 Testing PREPARATION PROCEDURES

45.6.1 Voting System Provider Demonstration SYSTEM PROVIDER DEMONSTRATION

45.6.1.1(A) The voting system provider shall demonstrate the exact proposed submitted voting system to the Secretary of State prior to any functional testing.

45.6.1.2(B) The demonstration period does not have a predetermined agenda for the voting system provider to follow; however, presentations should be prepared to address and demonstrate within the specific system, the following items as they pertain to each area and use within the voting system, IF APPLICABLE:

(a)(1) System overview;

(b)(2) Verification of complete system matching EAC certification;

(c)(3) Ballot definition creation;

(d)(4) Printing ballots on demand;

(e)(5) Hardware diagnostic testing;

(f)(6) Programming election media devices for various counting methods INCLUDING:

(i)(A) Mail-in Ballots;

(ii)(B) Early Voting;

(iii)(C) Precinct/Poll Place;

(iv)(E) Provisional; and

(v)(F) Vote Center.

(g)(7) Sealing and securing system devices;

(h)(8) Logic and accuracy testing;
(9) Processing ballots;

(10) Accessible use;

(11) Accumulating results;

(12) Post-election audit;

(13) Canvass process handling;

(14) Audit steps and procedures throughout all processes;

(15) Certification of results; and

(16) Troubleshooting.

45.6.1.3 (C) The voting system provider shall have access to the demonstration room for one day prior to the start of the demonstration to provide time for setup of the voting system.

45.6.1.4 (D) A maximum of one business day is normally allowed for the demonstration. If the voting system provider requests more time for the demonstration or, if the Secretary of State finds that the complexity of the system is such that more time is needed for a demonstration, more time may be granted.

45.6.1.5 (E) The demonstration shall be open to representatives of the press and the public to the extent allowable. The Secretary of State may limit the number of representatives from each group to accommodate space limitations and other considerations.

45.6.1.6 (F) The Secretary of State shall post notice of the fact that the demonstration will take place in the designated public place for posting such notices for at least seven days prior to the demonstration. The notice shall indicate the general time frame during which the demonstration may take place and the manner in which members of the public may obtain specific information about the time and place of the test.

45.6.1.7 (G) The voting system provider shall provide the same class of workstation and/or server for testing the voting system as the normal production environment for the State of Colorado.

45.6.2 Functional Testing

45.6.2.1 Voting system provider requirements for testing

45.6.2.1.1 (H) Based upon the review of VSTL or other state reports and test records, the Secretary of State will prepare a test plan. The test plan shall
be designed to test for any requirements specific to Colorado law which were not addressed in prior testing and for any federal or Colorado requirements which were not addressed to the satisfaction of the Secretary of State in the reports and records from prior testing.

45.6.2.1.2 (I) The test plan shall include the election definitions to be used in testing and specifications for test ballots. Test ballots and election definitions shall generally follow all requirements for election definitions, ballot layout and printing to verify the system’s ability to meet those requirements. Some election definitions and ballots may depart from the requirements in order to test specific functions.

45.6.2.1.3 (J) For each system tested, a requirements matrix shall be prepared to identify those requirements satisfied by the review of VSTL or other state reports and test data and how those requirements not satisfied are to be tested or otherwise satisfied. If during test planning or testing one of the requirements in the voting systems standards or in this rule are determined to be not applicable to the system under test, the reason for the determination will be documented.

45.6.2.1.4 (K) The voting system provider shall submit for testing the specific system configuration that will be offered to jurisdictions including the components with which the voting system provider recommends the system be used.

45.6.2.1.5 (L) The voting system provider is not required to have a representative present during the functional testing, but shall provide a point of contact for technical support. After the delivery, unpacking and initial inspection of the equipment for shipping damage and missing components, a vendor representative shall only be allowed to operate or touch the equipment when approved by the Secretary of State. All such activity by a vendor representative shall be documented on video and in writing.

45.6.2.1.6 (M) The proprietary software shall be installed on the workstation/server and all applicable voting system components by the Secretary of State or the VSTL using the trusted build and the installation procedures provided by the voting system provider. After installation, hash values for the software and firmware shall be compared to any published hash values of the trusted build. Any mismatches in hash values will be investigated and resolved before proceeding with testing.

45.6.2.1.7 (N) All equipment shall be hardened using the voting system provider’s procedures and specifications.

45.6.2.1.8 (O) Testing shall be performed with test election definitions and test ballots as required in the test plan.
45.6.2.1.9 (p) The results of all testing shall be recorded in the requirements matrix. The requirements matrix shall be the primary record describing which requirements were met and specifying which were not. It shall be supplemented as necessary to support the findings with test team notes and system reports. Supplemental information may include photographs and audio or video recordings.

45.6.2.1.10 (q) Functional testing shall be completed according to the phases identified in Rule 45.3.3.

45.6.2.2 Secretary of State requirements for testing

45.6.2.2.1 (r) The Secretary of State OR THE VSTL shall conduct functional testing on the voting system based on this Rule 45 and additional testing procedures as determined by the Secretary of State.

45.6.2.2.2 (s) The voting system shall receive a pass, fail or not applicable for each requirement with appropriate notation in the requirements matrix.

45.6.2.2.3 (t) Records of the test procedures shall be maintained and recorded on file with the Secretary of State IN ACCORDANCE WITH RULE 45.4.7. The records shall identify the system and all components by voting system provider name, make, model, serial number, software version, firmware version, date tested, test number, test plan, requirements matrix, test team notes and other supplemental information, and results of test. The test environment conditions shall be described.

45.6.2.2.4 (u) In the event that a deviation from the test plan is required, it shall be documented in a test team note. The note shall provide a description of the deviation, the reason for the deviation and effect of the deviation on testing and determining compliance with requirements.

45.6.2.3 45.6.2 General Testing Procedures and Instructions

AND INSTRUCTIONS

45.6.2.3.1 (A) Certification tests shall be used to determine compliance with applicable performance standards for the system and its components. The general procedure for these tests shall:

(a) (1) Verify, by means of the applicant’s voting system provider’s standard operating procedure, that the device is in a normal condition and status;

(b) (2) Establish the standard test environment or the special environment required to perform the test;

(c) (3) Invoke all operating modes or conditions necessary to initiate or to establish the performance characteristic to be tested;
(d)(4) Measure and record the value or the range of values of the performance characteristic to be tested; and

(e)(5) Verify all required measurements have been obtained, and that the device is still in a normal condition and status.

45.6.2.3.2(B) All tests shall be generally conducted in regular election mode. Tests of test mode and diagnostic functions may be conducted in the appropriate test mode.

45.6.2.3.3(C) The voting system provider is required to produce ballots and assemble marked test decks and spare ballots as specified in the test plan.

45.6.2.3.4 The voting system provider shall provide a minimum of ten ballot marking pens/pencils/markers as defined by their system for marking ballots by the Secretary of State.

45.6.2.3.5(D) For mark-sense or optical scan devices, the Secretary of State OR THE VSTL will prepare 100 or more test ballots with marking devices of various color, weight and consistency to determine the range of marks that can be read and the range and consistency of reading marginal marks.

45.6.2.3.6(E) Ballots shall be cast and counted in all applicable counter types (or counter groups) as necessary based on the parts included in the voting system. These are, at a minimum, Poll Place (or Vote Center), Mail-in, Provisional and Early Voting POLLING PLACE (OR VOTE CENTER), MAIL-IN, PROVISIONAL AND EARLY VOTING. Ballots may be run through components more than one time depending on components and counter group being tested to achieve a minimum number of ballots cast as follows for each group:

(a) Polling Place / OS = 1,000;

(b) Polling Place / DRE = 500;

(c) Vote Center and Early Voting EARLY VOTING / OS = 2,500;

(d) Vote Center and Early Voting EARLY VOTING / DRE = 500;

(e) Mail-in = 1, 500; and

(f) Provisional = 500.

45.6.2.3.7(F) Ballot design shall be sufficient to verify the scope of allowable ballot designs for the given system under Colorado election law.
45.6.2.3.8  Ballots shall be printed in applicable languages as required by state
or federal law, or both.

45.6.2.3.9  Ballots shall include candidates to represent the maximum number
of political parties in the State of Colorado, and shall accommodate all
qualified political parties and political organizations.

45.6.2.3.10(G) The requirements matrix shall include the following requirements
for election definitions and ballots to simulate and test “real world”
situations in the State of Colorado. Election definitions and ballots
shall include the following minimum contest criteria:

(a)(1) Parties for different races;

(b)(2) Selection of a pair of candidates;

(c)(3) In a Primary Election, allow voters to vote for
the candidates of the party for which they are eligible and for any
and all non-partisan candidates and measures, while preventing
them from voting on candidates of another party;

(d)(4) In a general election, allow a voter to vote for any candidate for
any office, in the number of positions allowed for the office, and to
vote for any measure on the ballot that the voter is allowed to vote
in, regardless of party;

(e)(5) Allow for programming to accommodate Colorado recall questions
as prescribed in Article 12 of Title 1, C.R.S.;

(f)(6) A minimum of 20 pairs of “yes” and “no” positions for
voting on ballot issues; and

(g)(7) Ability to contain a ballot question or issue of at least 200 words.

45.6.2.3.11  Additional tests and procedures may be requested at the discretion
of the Secretary of State.

45.6.2.3.12(H) A county clerk and recorder OR HIS/HER designated representative
may observe the functional testing of a voting system. The representative
may assist at the request of the Secretary of State. All such activity by a
county representative shall be documented on video and in writing.

45.6.2.3.13(I) The public shall be allowed to view all functional testing
conducted by the Secretary of State. However, legal limitations may
require that certain testing, including but not limited to proprietary
information and system security, be done outside the view of the public. If
the functional testing is outsourced to a testing lab or contractor, public
viewing shall be subject to limitations set forth by the testing lab or contractor.

45.6.2.3.14(J) If any malfunction or data error is detected, its occurrence and the duration of operating time preceding it shall be recorded for inclusion in the analysis and the test shall be interrupted. If corrective action is taken to restore the devices to a fully operational condition within eight hours, then the test may be resumed at the point of suspension.

45.6.3 The Secretary of State shall certify voting systems that substantially comply with the requirements in this Rule 45, Colorado Election Code, and any additional testing that is deemed necessary by the Secretary of State.

[Current Rule 45.6.3 moved to New Rule 45.3.4]

45.7 Temporary Use

45.7.1 If a voting system provider has a system that has not yet been approved for certification through the Secretary of State, the voting system provider or the designated election official may apply to the Secretary of State for temporary approval of the system to be used for up to one year.

45.7.2 Upon approval of temporary use, a jurisdiction may use the voting system, or enter into a contract to rent or lease the voting system for a specific election upon receiving written notice from the Secretary of State’s office. At no time shall a jurisdiction enter into a contract to purchase a voting system that has been approved for temporary use.

45.7.3 The Secretary of State shall approve use of a temporarily approved voting system for each election that a jurisdiction requests permission to conduct with the voting system.

45.7.4 Temporary use does not supersede the certification requirements and/or process, and may be revoked at any time at the discretion of the Secretary of State.

45.8 Periodic Review

45.8.1 The Secretary of State shall periodically review the voting systems in use in Colorado to determine if the system(s):

(a) Are defective, obsolete or unacceptable for use based on the requirements of this Rule 45; and

(b) Have been modified from certified and trusted build versions of hardware or software;
45.8.2 The Secretary of State shall review a minimum of two randomly selected jurisdictions and voting systems per calendar year at the choosing of the Secretary of State.

45.8.3 The Secretary of State shall conduct an annual visual inspection of all software incident records maintained by each voting system provider certified for use in the State of Colorado.

45.8.4 After such review, certification or temporary approval for use may be withdrawn. Three months notice shall be given prior to withdrawing certification of any voting system unless the Secretary of State shows good cause for a shorter notice period.

45.8.5 All forms, notes and documentation from a periodic review shall be kept on file with the Secretary of State.

[Current Rule 45.8 amended and moved to New Rule 11]

45.9 Decertification

45.9.1 If, after any time the Secretary of State has certified a voting system, it is determined that the voting system fails to substantially meet the standards set forth in this Rule 45, the Secretary of State shall notify any jurisdictions in the State of Colorado and the voting system provider of that particular voting system that the certification of that system for future use and sale in Colorado is to be withdrawn.

45.9.2 Certification of a voting system may be revoked and/or suspended at the discretion of the Secretary of State based on information that may be provided after the completion of the initial certification. This information may come from any of the following sources:

(a) The Election Assistance Commission (EAC);

(b) Voting System Test Laboratory (VSTL);

(c) The Federal Election Commission (FEC);

(d) The National Software Reference Library (NSRL);

(e) National Association of State Election Directors (NASED);

(f) The National Association of Secretaries of State (NASS);

(g) Information from any state elections department or Secretary of State;

(h) Information from Colorado County Clerk and Recorders or their association;
(i) Any other source the Secretary of State deems reliable.

45.9.3-45.8.3 If any voting system provider, provides for use, or installs, or causes to be
installed an uncertified or decertified voting system or component, the Secretary of
State may suspend use of the component or the voting system. [Section 1-5-
618(6), C.R.S.]

45.9.4-45.8.4 Pursuant to IN ACCORDANCE WITH section 1-5-621, C.R.S., the Secretary
of State shall hold a public hearing to consider the decision to decertify a voting
system.

45.10-45.9 Modifications and Re-examination REEXAMINATION.

45.10.1—Any modification, change or other alteration to a certified voting system
shall require certification or review of the modification under
section 1-5-618, C.R.S., unless the voting system provider decides to present the
modified system for certification under this Rule 45.

45.11 Acceptance Testing by Jurisdictions

45.11.1-45.10.1 Whenever an election—A jurisdiction acquires a new system or
modification of an existing system certified by the Secretary of State, VOTING
EQUIPMENT, the election jurisdiction shall perform acceptance tests of the system
before it may be used to cast or count votes at any election. The voting system
shall be operating correctly, pass all tests as directed by the acquiring
jurisdiction’s project manager or contract negotiator and shall be identical to the
voting system certified by the Secretary of State.

45.11.2-45.10.2 The voting system provider shall provide all manuals and training
necessary for the proper operation of the system to the jurisdiction, or as indicated
by their contract.

45.11.3-45.10.3 The election jurisdiction shall perform a series of functional and
programming tests that shall test FOR all functions of the voting system at their
discretion.

45.11.4—The jurisdiction shall coordinate acceptance testing with the Secretary of
State and complete a Jurisdiction Acceptance Test form provided by the Secretary
of State.

[Current Rule 45.11.4 amended and moved to New Rule 11]

45.12 Purchases and Contracts

45.12.1—Any voting system that has been certified under the procedures of this
Rule 45 are eligible for purchase, lease, or rent for use by jurisdictions within the
State of Colorado providing the contract contains the following items:
(a) The voting system is certified for use within the state;

(b) Contract contains training and maintenance costs for jurisdiction; and

(c) Contract identifies components contained in the certified voting system and appears complete with all accessories necessary for successfully conducting an election within the laws and rules of the State of Colorado.

45.12.2 The Secretary of State shall maintain on file a list of all components used and purchased for use. The list shall include, at a minimum, the name of the jurisdiction, the date of purchase, the serial number(s) of voting devices and name of the voting systems that was purchased.

45.13 Financial Statements of Voting System Providers

45.13.1 All voting system providers applying for certification in the State of Colorado, or doing business in the State of Colorado, shall provide quarterly financial statements and an annual auditor's report to the Secretary of State. All financial statements and reports shall be due:

(a) Prior to the completion of functional testing for any voting system being submitted for certification;

(b) At the conclusion of each accounting quarter for providers with equipment certified for use in the State of Colorado; and

(c) Upon issuance of a final auditor's report after the completion of each annual audit.

45.13.2 Financial statements submitted to the Secretary of State shall include a Statement of Cash Flow, Statement of Retained Earnings, Balance Sheet, and Income Statement.

[Current Rule 45.13 amended and moved to New Rule 11]

45.11 Escrow of Voting System Software by Voting System Provider

45.11.1 Voting System Providers—The voting system provider must place in escrow a copy of the election software, firmware, and supporting documentation being certified with either the Secretary of State or an independent escrow agent approved by the Secretary of State. See section [SECTION 1-7-511, C.R.S.]

45.11.2 Within ten days of the Voting System—Voting System provider receiving notification of examination of voting equipment as part of the certification process, the Voting System Provider shall arrange for the completion of escrow requirements as indicated by this rule.
11.8.3 45.11.3 Voting System Provider shall sign a sworn affidavit that the election software in escrow is the same as the election software used in its voting systems in this state. An annual update of the affidavit will be on file in a secured location with the Secretary of State’s office.

11.8.4 45.11.4 A complete copy of the certified election software including any and all subsystems of the certified software shall be maintained in escrow.

11.8.5 45.11.5 Any changes to current configurations or new installations must be approved through the certification program of the Secretary of State.

11.8.6 45.11.6 In addition to the requirements listed below, the Voting System Provider must include a cover/instructions sheet for any escrow material to include the Voting System Provider Name, Address, Software Version, Hardware Version, Firmware Revision Number, and other uniquely identifying numbers of the software submitted for certification.

11.8.7 45.11.7 Election Software Source Code, maintained in escrow, shall contain internal documentation such that a person reasonably proficient in the use of the programming language can efficiently use the documentation to understand the program structure, control techniques, and error processing logic in order to maintain the Source Code. Source Code should it be removed from escrow for any reason.

11.8.8 45.11.8 System documentation shall include instructions for converting the escrowed Source Code into Object Code, organized and configured to produce an executable system, if warranted.

11.8.9 45.11.9 System documentation shall include technical architecture design, analysis, detail design, testing and an installation and configuration guide.

11.8.10 45.11.10 A set of schematics and drawings on electronic vote casting and counting equipment purchased or in use by the county clerk and recorder shall be on file with the Secretary of State.

11.8.11 45.11.11 All parties shall treat as confidential the terms of this Section Rule including all escrow materials and any other related information that comes into their possession, control or custody pursuant to IN ACCORDANCE WITH this section.

11.8.12 45.11.12 Copies of Electronic media and supporting documentation for Escrow within the Secretary of State shall be sent to:

Colorado Secretary of State
Attn: Voting Systems Specialist
1700 Broadway – Suite 270-200
Denver, CO 80290
11.8.13 45.11.13 Any cost of using an alternative third party escrow agent shall be borne by the Voting System provider

[Current Rule 11.8 is amended and moved to New Rule 45.11. Modifications are shown above.]

Rule 46. RESERVED

Rule 47. RESERVED

Rule 48. RESERVED

Rule 49. RESERVED

Rule 50. RESERVED

Rule 51. Use of approved and recommended election forms

51.1 Where the Secretary of State has issued an approved election form, notice, application, or correspondence provided for by the “Uniform Election Code of 1992”, all designated election officials and registration offices shall use the approved form.

51.1.1 A designated election official or registration office that wishes to substantially modify the content of any form approved or recommended by the Secretary of State shall submit a written request via email to the Secretary of State’s office stating the requested modification and the reasons it is needed.

(a) The Secretary of State shall have WILL APPROVE A REQUEST TO modify an approved form within five business days. Failure of the Secretary of State to issue a decision within five business days shall DO NOT constitute an approval of the request. If the modification request is denied, the Secretary of State will provide an explanation stating the basis for denying the request.

(b) A non-substantive customization of an approved form, such as placing the form on county letterhead or language translation, does not require the Secretary of State’s approval.

51.2 The Secretary of State shall approve standard voter registration and ballot application forms recommended for use by political parties and organizations that provide such forms to the public. The Secretary of State will publish on the department’s website that the current approved registration forms for registration and ballot request are publicly available on its website.
51.2.1 Political parties and organizations may also use the National Mail Voter Registration form. Because the forms approved by the Secretary of State contain all of the information specific to SPECIFICALLY REQUIRED BY Colorado law, the applicants and the organization are afforded greater protection when BY DISTRIBUTING OR USING the standard STATE forms approved by the Secretary of State are used.

51.2.2 All political parties and organizations that conduct a mass mailing of either registration or ballot request forms to the public MUST identify the party or organization conducting the mailing THEMSELVES by printing the organization name and contact information on the form.

51.2.3 Any political party or organization may contact the Secretary of State prior to—BEFORE sending a mailing to request a review of the form and information to be mailed.

51.3 In accordance with UNDER section 1-1-107(2)(d), C.R.S., the Secretary of State may WILL seek injunctive action or other penalties as a remedy to REMEDIES FOR violations of this Rule.