Rule 21. Voting System Standards for Certification

21.1 Introduction

21.1.1 The standards for certifying a voting system in this Rule apply to applications for new certifications. Voting system providers may submit an application to modify a system previously certified by the Secretary of State in accordance with section 1-5-618, C.R.S.

(a) The Secretary of State will only approve an application for modification if testing determines that the changes proposed do not adversely affect any one or more of the following:

(1) Performance of voting system functions;

(2) Voting system security and privacy;

(3) Overall flow of system control; or

(4) The manner in which ballots are defined and interpreted, and voting data is processed.

(b) The Secretary of State may approve a test plan for a modified voting system limited to the correction of defects; the incorporation of improvements; the enhancement of portability and flexibility; and the integration or compatibility of data exported from the voting system with other elections systems.

(c) A voting system provider may apply for modification to a currently certified voting system to address de minimis commercial off-the-shelf hardware changes using the process laid out in this Rule.

(1) The provider must submit an application package that includes an application for modification provided by the Secretary of State, internal testing documentation, VSTL determination of de minimis changes, specification documents for existing and new equipment, updated TDP documents as applicable, other engineering change order documents, an integration testing plan, and any other documentation requested by the Secretary of State. If the submitted application package is incomplete the Secretary of State will identify the deficiencies and the voting system provider must remedy the deficiencies within ten days.

(2) If the Secretary of State reviews the application package and determines that the modification requires any additional testing from the VSTL, the provider will work with the Secretary of State to create a test plan for the modification. The Secretary of State makes the final determination as to whether the change is de minimis or not.

(3) If the Secretary of State reviews the application package and determines that the modification does not require testing by the VSTL, the provider will coordinate with the Secretary of State to perform integration testing overseen by the Secretary of State using the plan provided in the application package.

(4) Upon completion of testing the Secretary of State will review the outcomes of the integration testing and determine if the modification

complies with section 1-5-618(1.5), C.R.S. and approve or deny the modification request.

21.1.2 Sufficient components must 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.

21.1.3 The certification of a voting system is not 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 are exempted by law and choose to manually tabulate the election results.

21.1.4 A voting system vendor applying for certification or modification must notify the Secretary of State at the time of application if any component previously certified for use in Colorado is not included in the application for certification or modification.

21.2 Certification process overview and timeline

21.2.1 The voting system will be considered as a unit, and all components tested at once, unless the circumstances necessitate otherwise. Any change made to individual components of a voting system will require the entire voting system to be recertified unless the change is a modification that can be approved under section 1-5-618(1.5), C.R.S.

21.2.2 For a voting system to be certified, the voting system provider must successfully complete all phases of the certification process. The certification process includes: submission of a complete application, a documentation review, a public demonstration of the system,-functional testing, and escrow of state certified election software.

21.2.3 The flow of each phase of certification is as follows:

(a) Phase I – The voting system provider must submit an application with all documentation required in Rule 21.3 and a completed requirements matrix provided by the voting systems team. The Secretary of State will review the application and inform the voting system provider whether or not the application is complete. If the application is incomplete, the Secretary of State will 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 will review the submitted documentation, Colorado requirements matrix, VSTL reports from previous testing, and evaluations provided by other states. If the submitted documentation or requirements matrix is incomplete, the Secretary of State will identify the deficiencies and the voting system provider will have 30 days to remedy the deficiencies and make them complete.

(c) Phase III – The Secretary of State must approve a certification test plan. If a VSTL is contracted to test the voting system, the VSTL will work with the voting system provider to prepare a certification test plan. The certification test plan will be presented to the Secretary of State for review and approval.

(d) Phase IV– Upon receipt of the Secretary of State's approval of the certification test plan, the VSTL will execute the test plan.

(e) Phase V – The Secretary of State will review the test results and determine whether the voting system substantially meets the requirements for certification. Before the Secretary of State will make a final determination of whether the system substantially meets the requirements, the voting system provider must escrow in compliance with section 1-7-511, C.R.S. Within 30 days of a decision, the Secretary of State will post the certification test report for the voting system on its website.

21.2.4 The Secretary of State will certify voting systems that substantially comply with the requirements in this Rule 21, and any additional testing the Secretary of State finds necessary.

21.3 Application procedure

21.3.1 Any voting system provider that wants to apply for certification must communicate their timing and intent to apply with the voting systems team prior to submitting a complete application package. If the timing of the submission would present a hardship for the Secretary of State, the Secretary may request the provider to delay submission of the application to a later date agreed upon by all parties.

21.3.2 A voting system provider that desires to submit a voting system for certification must complete the Secretary of State's "Application for Certification of Voting System" that is available on the Secretary of State's website.

21.3.3 Along with the application, the voting system provider must submit all documentation required in the application for certification in a searchable electronic format. The Secretary of State may delay the certification process if the documentation is insufficient or incomplete until remedied by the voting system provider.

21.3.4 The voting system provider must submit the completed Colorado requirements matrix to the Secretary of State in a timely manner after submission of the application for certification.

(a) The voting system provider must specify where each requirement is met in the documentation, including section or page number.

(b) The voting system provider must specify which requirements will be fulfilled by testing instead of documentation.

(c) All requirements in the Colorado requirements matrix must be addressed.

21.3.5 The vendor must identify any material it asserts is exempt from public disclosure under the Colorado Open Records Act, Part 2, Article 72 of Title 24, C.R.S., together with a citation to the specific grounds for exemption before beginning Phase V of the certification process.

21.3.6 The voting system provider must coordinate with the Secretary of State for the establishment of the trusted build. The voting system provider must 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, the trusted build must include a compilation of files placed on write-once media, and an established hash file distributed from a VSTL or

the National Software Reference Library to compare federally certified versions. The trusted build disks should all be labeled with identification of the voting system provider's name and release version.

21.3.7 All materials submitted to the Secretary of State must remain in the custody of the Secretary of State 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.

21.4 Voting System Standards

21.4.1 The 2002 Voting Systems Standards are incorporated by reference. Material incorporated by reference in the Election Rules does not include later amendments or editions of the incorporated material. Copies of the material incorporated by reference may be obtained by contacting the Federal Election Commission, 999 E Street NW, Washington, DC, 20463, 800-424-9530.

21.4.2 All voting systems must meet the requirements of the 2002 Voting Systems Standards, parts 5 – 7 of article 5 of title 1, C.R.S., as amended, and this Rule 21.

21.4.3 The voting system provider must document that all voting system software, hardware, and firmware meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include:

(a) The Help America Vote Act,

(b) The Americans with Disabilities Act, and

(c) The Federal Rehabilitation Act.

21.4.4 Independent Analysis. Before completion of functional testing, all voting system providers submitting a voting system must complete an independent analysis of the system, which includes:

(a) An application penetration test conducted to analyze the system for potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The test must involve active exploitation of security vulnerabilities of the voting system according to a penetration test plan approved by the Secretary of State, whether or not the vulnerabilities can be mitigated through compensating controls.

(b) A source code evaluation conducted 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 approved after January 1, 2008.

(c) A complete report detailing all findings and recommended compensating controls for vulnerabilities and deficiencies identified.

(d) The voting system provider must use at least one of the following to perform the independent analysis:

(1) An EAC approved VSTL;

(2) An independent testing organization approved by the Secretary of State; or

(3) Testing conducted in another state.

(e) The Secretary of State or VSTL will 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.

(f) The Secretary of State may 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.

21.4.5 Functional Requirements

(a) Functional requirements must address all detailed operations of the voting system related to the management and controls required to successfully conduct an election.

(b) The voting system must provide for appropriately authorized users to:

(1) Set up and prepare ballots for an election;

(2) Lock and unlock system to prevent or allow changes to ballot design;

(3) Conduct hardware diagnostic testing;

(4) Conduct logic and accuracy testing;

(5) Conduct an election and meet requirements as identified in this Rule 21 for procedures for voting, auditing information, inventory control where applicable, counting ballots, opening and closing polls, recounts, reporting and accumulating results;

(6) Conduct the post-election risk-limiting audit; and

(7) Preserve the system for future election use.

(c) The voting system must integrate election day voting results with mail and provisional ballot results.

(d) The election management system must 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. The software must provide authorized users with the ability to generate these files on an “on-demand” basis. After creating such files, the authorized users must have the capability to copy the files to CD-ROM or removable media.

(1) Exports necessary for the Secretary of State must conform to a format approved by the Secretary of State. The format must be compatible with

a commercially available data management program such as a spreadsheet, database, or report generator.

(e) The election management system must ensure that an election setup record may not be changed once ballots are printed and/or election media devices are downloaded without proper authorization and acknowledgement by the application administrative account. The application and database audit transaction logs must accurately reflect the name of the system operator making the changes and the date and time of the changes. The application and database audit transaction logs must support user's ability to examine the "old" and "new" values of the changes.

(f) All BMD voting devices must use technology providing visual or auditory ballot display and selection methods used by people with disabilities.

(g) All electronic voting devices supplied by the voting system provider and used at voter service and polling centers must 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.

21.4.6 Physical and design characteristics

(a) Physical and design characteristics must address any and all external or internal construction of the physical environment of the voting system.

(b) The voting system provider must 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.

21.4.7 Ballot Definition Subsystem

(a) The ballot definition subsystem of the voting system application consists of hardware and software required to accomplish the functions outlined in this Rule.

(b) The ballot definition subsystem must be capable of handling at least 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.

(c) The voting system must accommodate single page ballots (races on one face or both faces) and two page paper ballots (races on three or four faces).

(d) The ballot 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;

(2) Generate all required masters and distributed copies of the ballot definition files; and

(3) Permit a user to program the election, build the election database, generate and layout ballots, and report results, by ballot style or precinct, as permitted or required by section 1-7.5-208, C.R.S.

(e) Data management applications that collect, convert, manage or export election definition information in one or more formats suitable for import into the election management system, are an essential component of, and must be integrated with and operate in the same user interface and on the same server or workstation, as the election management system.

(f) The voting system may not add any caption or endorsement to ballot artwork generated by the voting system, including without limitation copyright notices or the name of the voting system provider. The county must have the ability to suppress any captions and endorsements generated by the voting system that are not authorized by section 1-5-407(1), C.R.S.

21.4.8 Trusted Build. The voting system must allow the operating system administrative account to verify that the software installed is the certified software by comparing it to the trusted build or other reference information.

21.4.9 Audit capacity

(a) The voting system must track and maintain read-only audit information of the following election management system events:

(1) Log on and log off activity;

(2) Application start and stop;

(3) Printing activity, where applicable;

(4) Election events – set for election, unset for election, open polls, close polls, end election, upload devices, download devices, create ballots, create precincts, create districts, create voter service and polling centers, initialize devices, backup devices, and voting activity; and

(5) Hardware events – add hardware, remove hardware, initialize hardware, and change hardware properties.

(b) All transaction audit records of the election databases must be maintained in a file outside of or separate from the database in a read-only format.

21.4.10 Security requirements. All voting systems must meet the following minimum system security requirements:

(a) The voting system must meet the following requirements to accommodate a general system of access by least privilege and role-based access control:

(1) Operating system administrative accounts may not have access to read or write data to the database;

(2) Operating system user/operator accounts must be able to be created that are restricted from the following aspects of the operating system:

(A) No access to system root directory;

(B) No access to operating system specific folders;

(C) No access to install or remove programs; and

(D) No access to modify other user accounts on the system.

(3) Application administrative accounts must have full access and rights to the application and database;

(4) Application user/operator accounts must have limited rights specifically designed to perform functional operation within the scope of the application. This user/operator must be restricted in the creation or modification of any user/operator accounts.

(b) The voting system must meet the following requirements for network security:

(1) All network-applicable components of the voting system must have the ability to operate on a closed network dedicated to the voting system;

(2) All network-applicable components of the voting system must 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

(3) The voting system must include provisions for updating security patches, software and/or service packs without access to the open network.

(c) All voting systems that use databases must: Have databases hardened to specifications developed by the voting system provider. Documentation included with the application must provide a detailed procedure for hardening according to current industry standards. Any government or industry guidelines adopted in whole, or in part, are to be identified in the documentation.

(d) The voting system must meet the following requirements for operating system security:

(1) All voting systems must have all operating systems hardened to specifications developed by the voting system provider according to current industry standards. Documentation included with the application must provide a detailed procedure for hardening. Any government or industry guidelines adopted in whole, or in part, are to be identified in the documentation.

(2) The voting system provider must configure the voting system operating system of the workstation and server used for the election management software to the following requirements:

(A) The ability for the system to take an action upon inserting a removable media (auto run) must be disabled; and

(B) The operating system must only boot from the drive or device identified as the primary drive.

(3) The voting system provider must use a virus protection/prevention application on the election management server/workstations which must be capable of manual updates without the use of direct connection to the internet.

(e) The voting system must meet the following requirements for password security:

(1) All passwords must be stored and used in a non-reversible format;

(2) Passwords to the database must not be stored in the database;

(3) Password to the database must be owned and only known by the application;

(4) The application's database management system must require separate passwords for the administrative account and each operator account;

(5) The system must be designed in such a way to ensure that the use of the administrative account password is not required for normal operating functions;

(6) The system must allow users to change passwords;

(7) The use of blank or empty passwords must 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

(8) All voting systems must have all components of the voting system capable of supporting passwords of a minimum of eight characters, and must be capable of including numeric, alpha and special characters in upper case or lower case used in any combination.

(f) All modules of the system must meet the 2002 voting system standards requirements for installation of software, including hardware with embedded firmware:

(1) 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 must be made available as part of a source code review.

(2) Security features and procedures must be defined and implemented to prevent any changes of interpreted data files after the initial election testing of the final election definition Replacement of the interpreted data files with tested and approved files from the trusted build must be by authorized personnel before the election definition is finalized for an election.

(3) The introduction of interpreted data during execution must 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.

(4) The application must not allow users to open database tables for direct editing.

(g) All voting systems must meet the following minimum requirements for removable storage media with data controls:

(1) All data stored that includes ballot images, tally data, and cast vote records must be authenticated, encrypted or secured against tampering, and validated.

(2) All removable media, upon insertion on server and workstations hosting the elections management software, must automatically be scanned by antivirus software or secured against execution of unauthorized software.

21.4.11 Documentation Requirements

(a) The Secretary of State may rely upon the testing of a voting system performed by a VSTL or by another state upon satisfaction of the following conditions:

(1) The Secretary of State has access to any documentation, data, test case 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

(2) The Secretary of State has determined that the tests were conducted in accordance with appropriate engineering standards, 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.

(b) In addition to other documentation requirements in this Rule, the voting system provider must provide the following documents:

(1) Standard issue users/operator manual;

(2) System administrator's/application administration manual;

(3) Training manual and related materials;

(4) Election definition programming and diagnostics manuals; and

(5) A list of minimum services needed for the successful, secure and hardened operation of all components of the voting system.

(c) For the review of VSTL or other state testing copies of all VSTL or state qualification reports, test logs and technical data packages must be provided to the Secretary of State.

(1) The voting system provider must execute and submit any necessary releases for the applicable VSTL, state or EAC to discuss any and all procedures and findings relevant to the voting system 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 must provide a copy of the documentation to the Secretary of State.

(2) The voting system provider, the VSTL, the state or the EAC will identify to the Secretary of State any specific sections of documents for which they assert a legal requirement for redaction.

(d) The voting system provider must provide documentation specifying the steps and times required for charging batteries, and the time of battery operation for each

type of device they provide, assuming continuous use of the devices by voters during an interruption of normal electrical power.

(e) The Secretary of State will review submitted documentation to determine the extent to which the voting system has been tested to federal standards.

(f) Failure by the voting system provider to provide any documentation will delay processing the application and may be cause for denial of certification.

(g) The voting system must include detailed documentation, which includes the location and a description of the content of the of audit trail information throughout the system. The audit information applies to:

(1) Operating Systems (workstation, server, ballot scanner, and BMD);

(2) Election management system; and

(3) Election Tabulation Devices – ballot scanner.

(h) The voting system provider must provide documentation detailing voting system security. The documentation must contain configurations, properties and procedures to prevent, detect, and log changes to system capabilities for:

(1) Defining ballot formats;

(2) Casting and recording votes;

(3) Calculating vote totals consistent with defined ballot formats;

(4) Reporting vote totals;

(5) Altering of voting system audit records;

(6) Changing or preventing the recording of a vote;

(7) Introducing data for a vote not cast by a registered voter;

(8) Changing calculated vote totals;

(9) Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and

(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.

(i) The voting system provider must provide documentation detailing the security measures it has in place for all systems, software, devices that act as connectors (upload, download, and other programming devices) and any additional recommended security measures.

(j) For the purpose of evaluating software, the voting system provider must provide detailed information as to the type of hardware required to execute the software.

(k) The documentation supplied by the voting system must 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.

(l) The voting system provider must submit documentation containing a list of minimum equipment, services, and executables required to run the election management system.

21.4.12 Ballot-level Cast Vote Records and Exports. All voting systems certified by the Secretary of State for use in Colorado after January 1, 2016 must meet the following requirements for ballot-level cast vote records and exports:

(a) The voting system must capture a ballot-level cast vote record (CVR).

(b) The voting system must be able to aggregate in a single file and export all CVRs in comma-separated value (CSV) text format.

(c) The CVR export must contain the following fields, with values or data populated by the voting system:

(1) CVR Number. A sequential number from one to the number of CVRs in the export file. This can be used as an alternate method to identify each CVR.

(2) Batch ID. Identifies the batch in which the paper ballot corresponding to the CVR is located.

(3) Ballot Position. Identifies the position of the paper ballot corresponding to the CVR within the batch.

(4) Imprinted ID. If the scanner model supports imprinting a unique character string on the ballot during the scanning process, the voting system must populate this field with the unique character string.

(5) Ballot Style. Indicates the ballot style or type of the paper ballot corresponding to the CVR.

(6) Device or tabulator ID. Identifies the scanning device by device or tabulator ID.

(7) Contest and Choice Names. Each contest and choice on any ballot in the election must have its own field so that voters' choices in all contests can be easily and independently tabulated after the CVR export is imported into a spreadsheet application.

(8) Number of Valid Choices. The number of valid choices (e.g., "Vote for 3") for each contest.

(d) The header or field names in the CVR export must unambiguously correspond to names of the contests and choices on the paper ballots.

(e) The contests and choices must be listed in the same order as they appear on the ballots.

(f) A vote for a choice must be indicated by a “1”. No vote for a choice or an overvoted condition must be indicated by a “0”. Choices that are not applicable to the CVR must be left blank.

21.4.13 Election Night Reporting data and exports. All voting systems certified by the Secretary of State for use in Colorado after January 1, 2016 must meet the following requirements for Election Night Reporting data and exports:

(a) The voting system must be able to generate and export results data suitable for use in the Secretary of State’s Election Night Reporting (ENR) system, as specified in the remaining subsections of this Rule.

(b) The ENR export file must be in a tabular format that uses comma-separated value (CSV) format, or a format based on a range of character positions within a line.

(c) The ENR export file must contain a header line that defines all of the fields contained in the export file.

(1) The header names need not exactly correspond to the field names specified subsection (d) of this Rule, but must unambiguously identify the content of each field.

(2) The order of the fields within the export file may deviate from the order specified in subsection (d) of this Rule.

(3) Additional fields contained in the ENR export file but not specified or addressed in subsection (d) of this Rule must not contain only alphanumeric characters.

(d) The ENR export file must include the following items or fields:

(1) Precinct Name. If the county defines the election to report results by precinct, an alphanumeric string consisting of a 10-digit precinct code.

(2) Ballot Style Name. If the county defines the election to report results by ballot style or district, a unique, alphanumeric string for each ballot style.

(3) Precinct ID. If the county defines the election to report results by precinct, a unique integer for each precinct or precinct split.

(4) Registered Voters. The number of registered voters eligible to vote each unique ballot style, or in each precinct or precinct split, as applicable.

(5) Ballots counted. The number of ballots counted for each unique ballot style, or each precinct or precinct split, as applicable.

(6) Contest Name. The contest name as it appears on the ballots. If the contest name contains a carriage return for ballot formatting purposes, then the carriage return must not appear in the export.

(7) Contest ID. A unique integer for each contest.

(8) Contest Sequence Number. A unique integer that defines the sequence of contests as they appear on the ballots.

(9) Votes Allowed. The maximum number of choices that a voter may select in each contest (e.g., “Vote for 2”).

(10) Choice Name. The choice name as it appears on the ballots. Party affiliation may not be included in the choice name.

(11) Choice ID. A unique integer for each choice within a contest.

(12) Party Code. An indicator of party affiliation for each choice, if applicable.

(13) Vote Count. The total number of votes for each choice.

(14) Reporting Flag. The reporting flag field must contain a value of “0”.

(15) Precinct Sequence Number. A unique integer that defines the sequence of precincts.

(16) Choice Sequence Number. A unique integer that defines the sequence of candidates as they appear on the ballot.

21.4.14 Central Ballot Counting Functionality. All voting systems certified for use in Colorado by the Secretary of State after January 1, 2016, must meet the following functional requirements for centrally counting ballots:

(a) Digital Ballot Adjudication: The voting system must include a digital ballot adjudication software application, enabling election judges to resolve, adjudicate, and duplicate ballots with marginal or ambiguous voter markings digitally rather than manually.

(b) Ballot Scanners. The voting system must include central count ballot scanners equipped with automatic document feeders, enabling election judges to scan multiple ballots rather than a single ballot at a time.

21.5 Testing preparation procedures

21.5.1 Voting system provider demonstration

(a) The voting system provider must demonstrate the submitted voting system to the Secretary of State prior to certification of the voting system.

(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 the following items as they pertain to each area and use within the voting system, if applicable:

(1) System overview;

(2) Verification of complete system matching the Application for Certification of a Voting System;

(3) Ballot definition creation;

(4) Hardware diagnostic testing;

(5) Programming election media devices;

(6) Sealing and securing system devices;

(7) Logic and accuracy testing;

(8) Processing ballots;

(9) Accessible use, including a full demonstration of all functionality using accessible voter interface devices and the audio ballot. This includes a video submitted with the demonstration which shows:

(A) A demonstration of the full functionality of the voter interface devices available for use with a ballot marking device; and

(B) A demonstration of a voting session from beginning to end, which includes the audio which will accompany voting on a ballot marking device, and which describes the actions available to the voter to take at every step on the device. The demonstration must allow for an individual who is visually impaired to follow each step taken during a voting session.

(C) The Secretary of State may require a voting system which has been adopted for use to provide a demonstration which follows the requirements of this Rule.

(10) Accumulating results;

(11) Post-election audit;

(12) Audit steps and procedures throughout all processes; and

(13) Troubleshooting.

(c) At the time of application, the voting system provider must arrange a time with the Secretary of State to access the demonstration room to setup the voting system if the demonstration is to be in-person.

(d) A maximum of one business day is normally allowed for a in-person 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.

(e) An in-person demonstration will 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.

(f) The Secretary of State will post notice of the fact that the in-person demonstration will take place in the designated public place for posting such notices for at least seven days prior to the demonstration. The notice must 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.

(g) The Secretary of State may allow a virtual demonstration in lieu of the in-person demonstration. A virtual demonstration may be livestreamed or a submitted video.

(h) If the Secretary of State allows a livestream virtual demonstration in lieu of an in-person demonstration, then the Secretary will post notice of the livestream demonstration at least seven days prior to the demonstration. The notice must indicate the time and link for the demonstration.

(i) If the Secretary of State allows a submitted video demonstration in lieu of an in-person demonstration, then the Secretary of State will post notice and provide a link to the submitted video prior to certification of the voting system.

21.5.2 Certification testing

(a) The voting system provider must provide the same class of workstation and/or server for testing the voting system as the normal production environment for the State of Colorado.

(b) 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 will 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.

(c) The test plan must include the election definitions to be used in testing and specifications for test ballots. Test ballots and election definitions must 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.

(d) For each system tested, a requirements matrix must 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.

(e) The voting system provider must 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.

(f) The voting system provider is not required to have a representative present during the functional testing, but must 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 will only be allowed to operate or touch the equipment when approved by the Secretary of State.

(g) The proprietary software must be installed on the workstation/server and all applicable voting system components by the Secretary of State or the VSTL using the trusted build following the installation procedures provided by the voting system provider. After installation, hash values for the software and firmware must 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.

(h) All equipment must be hardened using the voting system provider's procedures and specifications.

(i) Testing must be performed with test election definitions and test ballots as required in the test plan.

(j) The results of all testing must be recorded in the requirements matrix. The requirements matrix will be the primary record describing which requirements were met and specifying which were not. It must 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.

(k) Functional testing must be completed according to the phases identified in Rule 21.2.3.

(l) The Secretary of State or the VSTL must conduct functional testing on the voting system based on this Rule.

(m) The voting system must receive a pass, fail or not applicable for each requirement with appropriate notation in the requirements matrix.

(n) The Secretary of State will maintain records of the test procedures in accordance with Rule 21.3.7. The records must 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 must be described.

(o) In the event that a deviation from the test plan is required, it must be documented in a test team note. The note must provide a description of the deviation, the reason for the deviation and effect of the deviation on testing and determining compliance with requirements.

21.5.3 General testing procedures and instructions

(a) Certification tests must be used to determine compliance with applicable performance standards for the system and its components. The general procedure for these tests will:

(1) Verify, by means of the voting system provider's standard operating procedure, that the device is in a normal condition and status;

(2) Establish the standard test environment or the special environment required to perform the test;

(3) Invoke all operating modes or conditions necessary to initiate or to establish the performance characteristic to be tested;

(4) Measure and record the value or the range of values of the performance characteristic to be tested; and

(5) Verify all required measurements have been obtained, and that the device is still in a normal condition and status.

(b) All tests will be generally conducted in regular election mode. Tests of test mode and diagnostic functions may be conducted in the appropriate test mode.

(c) The voting system provider must produce ballots and assemble marked test decks and spare ballots as specified in the test plan.

(d) For mark-sense or ballot scanner 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.

(e) Ballots must 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, in-person, mail, and provisional ballots. 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 counted as follows for each group:

(1) Polling location = 500;

(2) Mail = 1,500; and

(3) Provisional = 500.

(f) The requirements matrix must 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 must include the following minimum contest criteria:

(1) Parties for different races;

(2) Selection of a pair of candidates, such as President and Vice-President;

(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;

(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;

(5) Allow for programming to accommodate Colorado recall questions as prescribed in Article 12 of Title 1, C.R.S.;

(6) A minimum of 20 pairs of "yes" and "no" positions for voting on ballot issues; and

(7) Ability to contain a ballot question or issue of at least 200 words.

(g) A county clerk or his or her designated representative must be able to observe the functional testing of a voting system. The representative may assist at the request of the Secretary of State.

(h) The public must 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 VSTL or contractor, public viewing is subject to limitations set forth by the VSTL or contractor.

(i) If any malfunction or data error is detected, its occurrence and the duration of operating time preceding it must be recorded for inclusion in the analysis.

21.6 Temporary use

21.6.1 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.

21.6.2 Temporary use does not supersede the certification requirements or process, and may be revoked at any time at the discretion of the Secretary of State.

21.6.3 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 may a jurisdiction enter into a contract to purchase a voting system that has been approved for temporary use.

21.7 Decertification

21.7.1 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 21, the Secretary of State will 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.

21.7.2 Certification of a voting system may be revoked 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 clerks or their association; or

(i) Any other source the Secretary of State finds reliable.

21.7.3 The Secretary of State may investigate a complaint filed by any person, and, upon any findings as outlined in (a) through (e) below, may prohibit, limit or decertify use of a voting system, in whole or in part. An investigation by the Office of the Secretary of State may include, but is not limited to, the review or inspection of the voting system component at issue.

(a) Any person installed any uncertified or decertified voting system component;

(b) A county breaks the chain-of-custody for any component of a voting system by allowing any individual not authorized by Rule 20.5.2(b) access to that component;

(c) A county submits an incident report regarding a component of a voting system and the Secretary of State finds that the chain-of-custody cannot be reestablished securely;

(d) A component of a voting system experiences repeated hardware failures or malfunctions of a similar nature; or

(e) The Secretary determines that the integrity or security of a voting system component cannot be verified and that chain-of-custody cannot be reestablished securely.

21.7.4 The Secretary of State will notify a county of the prohibition or limitation on use or decertification of a component of a voting system under Rule 21.7.3 and the county must immediately cease using that component.

21.7.5 In accordance with section 1-5-621, C.R.S., the Secretary of State will hold a public hearing to consider the decision to decertify a voting system if a political subdivision or provider of a voting system that is decertified has requested in writing that the Secretary of State reconsider.

21.7.6 If any voting system currently certified in Colorado is not used by any political subdivision for two consecutive general elections, the system may be decertified for use.

21.8 Modifications and reexamination. Any modification, change or other alteration to a certified voting system requires 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.

21.9 Acceptance Testing by Jurisdictions

21.9.1 Whenever a jurisdiction acquires voting equipment, the jurisdiction must perform acceptance tests of the system before it may be used to cast or count votes at any election. The voting system must be operating correctly, pass all tests as directed by the acquiring jurisdiction’s project manager or contract negotiator and must be identical to the voting system certified by the Secretary of State.

21.9.2 The voting system provider must provide all manuals and training necessary for the proper operation of the system to the jurisdiction.

21.9.3 The election jurisdiction must perform functional and programming tests for all functions of the voting system at their discretion.

21.10 Escrow of voting system software and firmware by voting system provider. The voting system provider must meet the requirement for election management software escrow per the following:

21.10.1 The voting system provider must place in escrow a copy of the election management software, firmware, and supporting documentation being certified with an independent agent approved by the Secretary of State.

21.10.2 The voting system provider must sign a sworn affidavit that the election management software in escrow is the same as the election management software used in its voting systems in this state.

21.10.3 A complete copy of the certified election management software including any and all subsystems of the certified software will be maintained in escrow.

21.10.4 Any changes to current configurations or new installations must be approved through the certification program of the Secretary of State.

21.10.5 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, address and pertinent contact information, software version, hardware version, firmware revision number, and other uniquely identifying numbers of the software submitted for certification.

21.10.6 Election management software source code, maintained in escrow, must 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.

21.10.7 System documentation will include instructions for converting the escrowed source code into object code, organized and configured to produce an executable system, if warranted.

21.10.8 All parties must treat as confidential the terms of this Rule including all escrow materials and any other related information that comes into their possession, control or custody in accordance with this section.

21.10.9 The provider must notify that Secretary of State via email that the election management software being certified has been placed in escrow.

21.10.10 Any cost of using an alternative third party escrow agent must be borne by the voting system provider.

21.11 Standards for certifying instant runoff voting functionality

21.11.1 Results reporting requirements

(a) The voting system must be capable of generating a summary report that lists the total number of votes for each candidate in each round. The report must include:

(1) The number of overvotes;

(2) Duplicate rankings;

(3) Skipped rankings; and

(4) Ballots with fewer rankings than the maximum permitted in the race.

(b) The voting system must generate a ballot image report, which can be fulfilled by exporting a cast vote record, that lists the order in which the elector ranked the candidates for each ballot.

(c) The voting system must generate a comprehensive report listing the results in the summary report by precinct or ballot style as required or permitted by section 1-7.5-208(3)(a), C.R.S.

21.11.2 Data export formats

(a) The voting system must accurately export complete round by round results data for use with an election night reporting system in .csv, .json, and .xml formats.

(b) The voting system must accurately export a cast vote record in .csv, .json, and .xml formats.

21.11.3 Ballot layout requirements

(a) The voting system must permit the user to lay out ballot cards containing both plurality and instant runoff voting contests on the same ballot card or separate ballot cards.

(b) The voting system must permit a user to input ranked voting specific voter instructions immediately preceding instant runoff voting contests.

(c) The voting system must be able to support ranking at least ten named candidates and up to two write-in candidates per instant runoff contest.

(d) The voting system must allow the ranked voting contests to be formatted on paper ballots in the following ways:

(1) Candidates listed in columns and rankings listed in rows.

(2) Rankings listed in columns and candidates listed in rows.

21.11.4 Tabulation requirements

(a) The voting system must record all voter rankings.

(b) During the first round of tabulation, the voting system must tabulate the first-choice ranks on each ballot.

(1) A candidate who receives over 50 percent of the first-choice ranks for a contest across all ballots tabulated is the winning candidate, and the voting system must stop tabulating any further rounds.

(2) If no candidate receives over 50 percent of the first-choice ranks for a contest across all ballots tabulated, the voting system must continue to the next round of tabulation

(c) During the next round of tabulation, the voting system must ensure that the candidate with the fewest first-choice ranks in the first round is eliminated, and

the eliminated candidate's votes are transferred to each ballot's next-ranked continuing candidate.

(1) If, after receiving the transferred votes, a continuing candidate receives over 50 percent of the votes cast on active ballots, that candidate is the winning candidate, and the voting system must stop tabulating any further rounds.

(2) If no candidate has over 50 percent of the votes cast on active ballots after the second round, the voting system must repeat additional rounds of tabulation as described in this Rule, until there is a winning candidate.

(d) If the combined votes of two or more candidates with the lowest vote totals in the current round are less than the number of votes for the continuing candidate with the next-highest number of votes, then the voting system must eliminate the group of lowest-vote candidates simultaneously.

(e) In any round, if two or more candidates tie for the lowest number of votes, and the voting system cannot eliminate the candidates according to the criterion in subsection (d), then the voting system must allow the user to determine by lot which candidates are eliminated in accordance with Rule 26.5.5.

(f) The voting system must allow the user to decide whether to allow skipped rankings or to exhaust the ballot when a ranking is skipped.

(g) The voting system must allow the user to decide if a vote for a non-certified write-in will exhaust the ballot or be resolved as a skipped ranking.

(h) The voting system must allow the user to decide whether to pause the tabulation session after each round or to continue until a winner is determined or a manual tie break for elimination is required.

(i) The voting system must allow the user to decide whether or not to include as an overvote ranks for candidates for whom votes may not be counted, in accordance with section 1-4-1001, C.R.S.

(j) The voting system must allow the user to decide whether to count a ranking for a candidate for whom votes may not be counted, in accordance with section 1-4-1001, C.R.S., as a skipped ranking or to elevate lower rankings.

21.11.5 Ballot marking device requirements

(a) Ballot marking devices must prohibit voters from overvoting any ranking.

(b) Ballot marking devices must prohibit voters from skipping rankings.

(c) The voting system must present clear audio and visual notifications if the voter has ranked fewer candidates than the contest's maximum permitted number of rankings but will allow the voter to proceed with their voting session if the voter chooses to do so.

21.11.6 Ballot adjudication requirements

(a) The voting system must allow the user to queue ballots with the following conditions for adjudication by election judges:

(1) Any ambiguous mark in any ranking;

(2) Any ranking that results in an overvote;

(3) Any skipped ranking;

(4) Any duplicate ranking; and

(5) Any contest in which a voter has ranked fewer candidates than the contest's maximum permitted number of rankings.