COLORADO SECRETARY OF STATE

8 CCR 1505-1

ELECTION RULES

Revised Draft of Proposed Revisions to Rule 45

January 12, 2007

This draft is not yet final. The proposed changes to be considered at the public rulemaking hearing may be different than the proposed changes in this draft. This is the current working draft of the revisions and amendments to Election Rule 45.

A final copy of the proposed rule changes will be available to the public no later than February 1, 2007, and a copy will be posted on the Department of State's web site, in compliance with the requirement of section 24-4-103(4)(a), C.R.S., that "[a]ny proposed rule or revised proposed rule by an agency which is to be considered at the public hearing . . . shall be made available to any person at least five days prior to said hearing."

Proposed additions or deletions from the initial draft are reflected using the "Track Changes" function. Proposed additions are reflected in SMALL CAPS *and* underlined*. Proposed deletions are shown in* ~~stricken type~~*. Annotations are included.*

1   **Rule 45. Rules Concerning Voting System Standards for Certification**

2   45.1   Definitions   The following definitions apply to their use in this rule only, unless otherwise
3   stated.

4   45.1.1 "Audio ballot" means a voter interface containing the list of all candidates, ballot
5   issues, and ballot questions upon which an eligible elector is entitled to vote at an
6   election and that provides the voter with audio stimuli and allows the voter to
7   communicate intent to the voting system through vocalization or physical actions.

8   45.1.2 "Audit log" means a system-generated record, in printed format, providing a record of
9   activities and events relevant to initialization of election software and hardware,
10   identification of files containing election parameters, initialization of the tabulation
11   process, processing of voted ballots, and termination of the tabulation process.

12   45.1.3 "Ballot image" or "Ballot image log" means a corresponding representation in
13   electronic form of the marks or vote positions of a cast ballot that are captured by a
14   direct recording electronic voting device.

15   45.1.4 "Ballot style assignment" means the creation of unique, specific ballots for an election
16   by the election management system based on criteria keyed into the system for

districts, precincts, and races to create combinations of possibilities of races for individual voters to choose based on their individual precincts.

45.1.5 "CLOSED NETWORK" MEANS A NETWORK STRUCTURE WHERE DEVICES ARE NOT CONNECTED TO ANY OTHER DEVICE EITHER SUPPORTED BY OR NOT SUPPORTED BY THE VOTING SYSTEM.

45.1.56 "Communications devices" means devices that may be incorporated in or attached to components of the voting system for the purpose of transmitting tabulation data to another data processing system, printing system, or display device.

45.1.67 "DRE" means a direct recording electronic voting device. A DRE is a voting device that records votes by means of AN AUDIO BALLOT OR ballot display provided with mechanical or electro-optical components that can be activated by the voter; that processes data by means of a computer program; and that records voting data and ballot images in memory components OR OTHER MEDIA. THE DEVICE MAY produce Aa 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.

45.1.78 "EAC" means the United States Elections Assistance Commission.

45.1.89 "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 needs required by the voting system for a particular election function. The election management system typically delivers (downloads) ballot style information to the election media and receives (uploads) cast ballot information in the form of a summary of results and ballot images.

45.1.910 "Equipment" or "device" means a complete, 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, as well as a complete end to end voting system solution.

45.1.1011 "FEC" means the Federal Election Commission.

45.1.1112 "ITA" means an independent test authority that provides engineering, testing, or evaluation services, and is certified by the National Association of State Election Directors (NASED) as qualified BY THE EAC to conduct qualification testing on a voting system.

45.1.12 "NASED" means the National Association of State Election Directors.

45.1.1313 "Remote site" means any physical location identified by a Designated Election Official as a location where the jurisdiction shall be conducting the casting of ballots
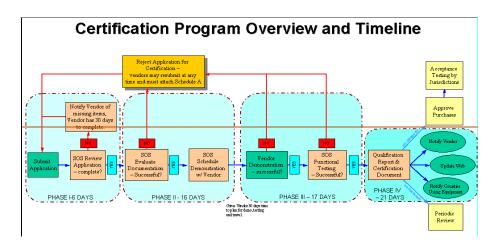
for a given election. A remote site includes locations such as precinct polling places, vote centers, early voting, absentee ballot counting, etc.

45.1.14   "REMOVABLE STORAGE MEDIA" MEANS ANY DEVICE THAT IS INTENDED TO BE REMOVED THAT HAS THE ABILITY OF STORING OR PROCESSING DATA FOR VOTING SYSTEM.

45.1.15   "SECURITY" MEANS THE ABILITY OF A SYSTEM TO PROTECT ELECTION INFORMATION AND ELECTION SYSTEM RESOURCES WITH RESPECT TO CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY.

45.1.16   "SPLIT PRECINCT" MEANS A PRECINCT THAT HAS A GEOGRAPHICAL DIVIDE BETWEEN ONE OR MORE POLITICAL JURISDICTIONS WHICH MAY CAUSE A UNIQUE BALLOT STYLE TO BE CREATED FOR A SPECIFIC ELECTION.

45.1.17   "TEST LOG" MEANS DOCUMENTATION OF CERTIFICATION TESTING AND PROCESSES WHICH IS INDEPENDENTLY REPRODUCIBLE TO RECREATE ALL TEST SCENARIOS CONDUCTED BY THE TESTING BOARD. THE LOG MAY INCLUDE DOCUMENTATION INCLUDING PHOTOGRAPHS, WRITTEN NOTES, VIDEO AND/OR AUDIO RECORDED NOTES IN AN EFFORT TO PROVIDE DETAIL TO THE TESTING SCENARIO INCLUDING OBSERVATION AND RESULTS.

45.1.18   "TRUSTED BUILD" MEANS THE INSTALLATION DISK FOR SOFTWARE AND FIRMWARE FOR WHICH THE SECRETARY OF STATE OR HIS/HER AGENT HAS ESTABLISHED THE CHAIN OF CUSTODY TO THE BUILDING OF A DISK, USED TO ESTABLISH AND/OR RE-ESTABLISH THE CHAIN OF CUSTODY AND OWNERSHIP OF ANY COMPONENT OF THE VOTING SYSTEM.

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, such as a precinct tabulation device, meets the definition of a voting system. Sufficient components shall be assembled to create a configuration that shall allow the system as a whole to meet all the requirements described for a voting system in this rule.

45.2.1.2 SUFFICIENT COMPONENTS SHALL BE ASSEMBLED TO CREATE A CONFIGURATION THAT SHALL ALLOW THE SYSTEM AS A WHOLE TO MEET ALL THE REQUIREMENTS DESCRIBED FOR A VOTING SYSTEM IN THIS RULE.

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.
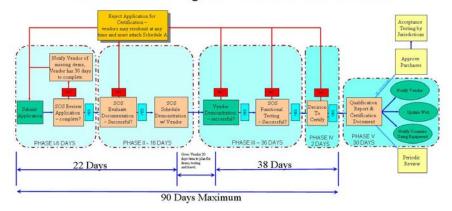
1   45.2.2.2 Certifications issued prior to this date shall be considered valid provided the
2   voting system meets the requirements of HAVA section 301(a).

3   45.3   Certification Process Overview and Timeline

4   45.3.1 The voting system shall be considered as a unit, and all components of such system
5   shall be tested at once, unless the circumstances necessitate otherwise (e.g. retrofitted
6   V-VPATs, etc.). Any change made to individual components of a voting system shall
7   require re-certification of the voting system in accordance with this rule.

8   45.3.2 For a voting system to pass certification the voting system provider shall successfully
9   complete all phases of the certification process that shall include: submitting a
10   complete application, successful review of the documentation to evaluate if the system
11   meets the requirements of this rule, successful demonstration of the system, followed
12   by successful completion of items determined mandatory in the functional testing
13   section of this rule.

14   45.3.3 The following milestones indicate the flow of the certification process – see timeline
15   below:

16   (a) Phase I – 6 days maximum. Voting system provider submits application and SOS
17   reviews for completeness. Voting system provider shall have 30 days to remedy
18   and make application complete.

19   (b) Phase II – 16 Days maximum. SOS evaluates the documentation submitted and
20   upon successful completion makes arrangement with voting system provider for
21   demonstration.

22   (c) Phase III – ~~17~~ 36 days maximum. When demonstration is complete, SOS performs
23   the functional testing.

24   (d) Phase IV – 2~~1~~ days maximum. Upon completion of functional testing, SOS
25   ~~produces a qualification report~~ MAKES A DECISION TO CERFITY A VOTING SYSTEM
26   and PRODUCES applicable certification document.

27   (E) PHASE V – 30 DAYS MAXIMUM. UPON DECISION TO CERTIFY A VOTING SYSTEM, SOS
28   PRODUCES A QUALIFICATION REPORT FOR THE VOTING SYSTEM AND COMPONENTS
29   CERTIFIED.
30

Certification Program Overview and Timeline

Certification Program Overview and Timeline

1
2

1 45.4   Application Procedure

2   45.4.1 Any voting system provider may apply to the SOS for certification at any time.

3   45.4.2 A voting system provider that submits a voting system for certification shall complete
4   the SOS's "Application for Certification of Voting System".

5   45.4.3 THE VOTING SYSTEM PROVIDER SHALL ESTABLISH AN ESCROW ACCOUNT PURSUANT TO
6   STATE PROCUREMENT PROCESSES TO COMPENSATE THE SOS FOR NECESSARY OUTSIDE
7   COSTS ASSOCIATED WITH THE TESTING OF THE SYSTEM. THE SECRETARY OF STATE
8   SHALL PROVIDE AN ESTIMATE OF COSTS FOR CERTIFICATION TESTING AT THE
9   CONCLUSION OF PHASE II EVALUATION. [CRITERIA TO BE DEVELOPED]

10   45.4.3̶4   Along with the application, the voting system provider shall submit all the
11   documentation necessary for the identification of the full system configuration
12   submitted for certification. This documentation shall include information that defines
13   the voting system design, method of operation, and related resources. It shall also
14   include a system overview and documentation of the voting system's functionality,
15   accessibility, hardware, software, security, test and verification specifications,
16   operations procedures, maintenance procedures, and personnel deployment and
17   training requirements. In addition, the documentation submitted shall include the
18   voting system provider's configuration management plan and quality assurance
19   program.

20   45.4.4̶5   Where applicable, electronic copies of documentation are preferred and may be
21   submitted in lieu of a hard copy.

22   45.4.5̶6   All materials submitted to the SOS shall REMAIN IN THE CUSTODY OF THE SOS
23   DURING THE LIFE OF THE CERTIFICATION AND FOR 25 MONTHS AFTER THE LAST
24   ELECTION IN WHICH THE SYSTEM IS USED become the property of the SOS upon
25   submission.

26   45.4.6̶7   In addition to the application and the documentation specified above, the SOS
27   may request additional information from the applicant, as deemed necessary by the
28   SOS.

29 45.5   Voting System Standards

30   45.5.1 Federal Standards

31   45.5.1.1 Pursuant to section1-5-601.5, C.R.S., and Rule 37.3, any voting system and
32   voting equipment offered for sale on or after May 28, 2004 shall meet the
33   voting systems standards promulgated in 2002 by the FEC and that may
34   hereafter be promulgated by the EAC.

35   45.1̶5.1.2   All voting system software, hardware, and firmware shall meet all
36   requirements of Federal law that address accessibility for the VOTER

INTERFACE OF THE voting system. These laws include, but are not necessarily 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 acknowledge explicitly that their proposed software, hardware, and firmware are all in compliance with the relevant accessibility portions of these laws.

45.5.1.3 THE VOTING SYSTEM PROVIDER SHALL DIRECT THE ITA OR THE EAC TO PROVIDE DOCUMENTATION INDICATING THE SUCCESSFUL COMPLETION OF ALL NECESSARY ITA TESTING BASED ON FEDERAL REQUIREMENTS. FAILURE TO PROVIDE DOCUMENTATION OF INDEPENDENT TESTING AS DEFINED BY THE EAC WILL RESULT IN THE VOTING SYSTEM APPLICATION BEING REJECTED.

45.5.2 State Standards

45.5.2.1 Functional requirements

45.5.2.1.1 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 The Voting system shall PROVIDE FOR APPROPRIATELY AUTHORIZED USERS TO have the functional capabilities to:

> **Formatted:** Small caps

(a) Prepare the system for an election;

(b) Setup and prepare ballots for an election;

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

(d) Conduct hardware and diagnostics testing as required herein,;

(e) Conduct logic and accuracy testing as required herein,;

(f) Conduct an election and meet additional requirements as identified in this section for procedures for voting, auditing information, inventory control, counting ballots, opening and closing polls, recounts, reporting, and accumulating results as required herein,;

(g) Conduct the post election audit as required herein; and

(h) Preserve the system for future election use.

45.5.2.1.3   The voting system shall ~~easily and~~ accurately integrate election day voting results with absentee, early voting as well as 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 voting of multiple ballot styles for a single precinct and~~ 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   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 a different ballot style.

45.5.2.1.7   The voting system shall provide authorized users with the capability to produce electronic files in ASCII (both comma-delimited and fixed-width) 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, or CD-ROM or to transmit the files to another information system.

45.5.2.1.8   The voting system shall include hardware and software to enable the closing of the voting location and disabling acceptance of ballots on all vote tabulation devices to allow for the following:

(a)   Machine-generated paper record of the time the voting system was closed.

(b)   Readings of the public counter and/or protective counter shall become a part of the paper audit record upon disabling the voting system to prevent further voting.

(c)   Ability to print an Abstract of the count of votes to contain:

(i)   Names of the offices

(ii)   Names of the candidates and party when applicable

(iii) A tabulation of votes from ballots of different political parties at the same voting location in a primary election

(iv) Ballot titles

(v) Submission clauses of all initiated, referred or other ballot issues

(vi) The number of votes counted for or against each candidate or ballot issue.

(d)   Abstract shall include a Judge's certificate and statement that contains:

(i)   Date of election (day, month and year)

(ii)   Precinct Number (ten digit format)

(iii) County or Jurisdiction Name

(iv)   State of Colorado

(v)   Count of votes as indicated in this section

(vi)   Area for judge's signature with the words similar to: "Certified by us", and "Election Judges". Space should allow for a minimum of two signatures.

(e)   Votes counted by a summary of the voting location, and by individual precincts.

(f)   Allow for multiple copies of the unofficial results at the close of the election.

45.5.2.1.9   Voters voting on DRE devices 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   The system shall ensure that an election setup may not be changed once ballots are printed and/or device media is downloaded for votes to be conducted without proper authorization and acknowledgement by a THE system APPLICATION administrator ADMINISTRATIVE ACCOUNT AND (B) THAT THE APPLICATION AND DATABASE AUDIT TRANSACTION LOGS ACCURATELY REFLECT THE NAME OF THE USER MAKING THE

Formatted: Small caps

Formatted: Small caps

Formatted: Small caps

CHANGE(S), THE DATE AND TIME OF THE CHANGE(S), AND THE
"OLD" AND "NEW" ~~vlues~~values of the change(s).

45.5.2.1.11 ~~The system shall be able to receive programming information from the Statewide Voter Registration System in XML format.~~

45.5.2.1.1~~1~~2 The system shall be able to export election results in either a web based format, or a~~N~~ ASCII (COMMA DELIMITED AND FIXED-WIDTH) FORMAT FOR USE IN OTHER APPLICATIONS. ~~delimited file (text, CSV, etc.) for use in other applications.~~

   (a) Exports necessary for the SOS shall conform to ~~XML~~ AN AGREED UPON format.

   (b) Export files shall be generated so that election results can be communicated to the SOS ON ELECTION NIGHT BOTH DURING THE ACCUMULATION OF RESULTS AND AFTER ALL RESULTS HAVE BEEN ACCUMULATED.

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 following minimum requirements for casting ballots:

   (a) Optical Scan Ballots at voting location(s) = 100 ballots per hour

   (b) DRE / Touch Screen = 20 ballots per hour

   (c) Central Count Optical Scan Ballots = 100 ballots per hour

[Comment: It may be necessary to establish baseline criteria regarding ballot size because of the growing length of the ballot, Particularly for the DRE where the length of the ballot may reduce the throughput.]

45.5.2.2.3 For the purposes 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. The performance level shall be such that a user of the software would have minimal pauses in the system during the ballot design and creation, along with the downloading and uploading of election media devices. Specifically, the following minimum standards are required:

(a)   Ballot style assignment is less than 10 seconds per ballot style

(b)   Election Media Download is less than 35 seconds per media

(c)   Election Media Upload is less than 20 seconds per media

(d)   View Ballot image (on screen) is less than 30 secONDS. per ballot image

45.5.2.2.4   At no time shall third party hardware or software impact performance levels, unless a voting system provider specifically details through documentation the specific hardware or software, the performance impact, and a workaround for the end user to overcome the issue.

45.5.2.3 Physical and Design Characteristics

45.5.2.3.1   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 functioning of the voting system to accomplish the successful conduct of an election on the voting system.

45.5.2.3.2   The physical design of the proposed system (non-software) shall be in a way such that it enhances or assists in the "voter friendly" aspect of voting, as well as meets the requirements indicated in section 4 of the "Usability and Accessibility of Voting Systems and Products" study conducted by NIST. (A copy of the document is located on the SOS web site.)

45.5.2.3.3   The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges:

(a)   Operating – Max. 100 95 Degrees Fahrenheit; Min 40 50 Degrees Fahrenheit, with max. humidity of 90%, normal or minimum operating humidity of 15%.

(b)   Non-Operating – Max. 130 140 Degrees Fahrenheit; Min. -15 4 Degrees Fahrenheit. Non-operating humidity ranges from 5% to 90% for various intervals throughout the day. The material 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

1   system.

2   45.5.2.3.4   The ballot definition subsystem of the voting system consists of
3   hardware and software required to accomplish the functions
4   outlined in this section 45.5.2.3. System databases contained in
5   the Ballot Definition Subsystem may be constructed
6   individually or they may be integrated into one database. These
7   databases are treated as separate databases to identify the
8   necessary types of data that shall be handled and to specify,
9   where appropriate, those attributes that can be measured or
10   assessed for determining compliance with the requirements of
11   this standard.

12   45.5.2.3.5   The Ballot Definition Subsystem shall be capable of formatting
13   ballot styles in multiple languages, including English and
14   SpanishAND ANY ADDITIONAL LAGUAGES AS ARE NECESSARY TO
15   COMPLY WITH THE "VOTING RIGHTS ACT OF 1965" 42 U.S.C. §
16   1973C ET SEQ. (1965). The subsystem shall be capable of being
17   updated to format ballot styles in additional languages as MAY
18   BECOME necessary under state or federal law.

19   45.5.2.3.6   The voting system shall allow the user to generate and maintain
20   an administrative database containing the definitions and
21   descriptions of political subdivisions and offices within the
22   jurisdiction.

23   45.5.2.3.7   The ballot definition subsystem shall provide for the definition
24   of political and administrative subdivisions where the list of
25   candidates or contests may vary within the remote site and for
26   the activation or exclusion of any portion of the ballot upon
27   which the entitlement of a voter to vote may vary by reason of
28   place of residence or other such administrative or geographical
29   criteria. This database shall be used by the system with the
30   administrative database to format ballots or edit formatted
31   ballots within the jurisdiction.

32   45.5.2.3.8   For each election, the subsystem shall allow the user to generate
33   and maintain a candidate and contest database and provide for
34   the production or definition of properly formatted ballots and
35   software.

36   45.5.2.3.9   The environment in which all databases in the subsystem are
37   maintained shall include all necessary provisions for security
38   and access control. Any database may be generated and
39   maintained in any file structure suitable to the requirements of
40   the end user. It shall be the intent of the database hierarchy

Formatted: Small caps

Formatted: Small caps

Formatted: Font: (Default) Times New Roman, 12 pt, Font color: Black, Small caps

Formatted: Small caps

Formatted: Small caps

1   ~~described herein to ensure that data entry, updating, and~~
2   ~~retrieval be effectively integrated and controlled.~~

3   45.5.2.3.9 The ballot definition subsystem shall be capable of handling at
4   least 500 potentially active voting positions, arranged to identify
5   party affiliations in a primary election, offices and their
6   associated labels and instructions, candidate names and their
7   associated labels and instructions, and issues or measures and
8   their associated text and instructions.

9   45.5.2.3.10 The ballot display may consist of a matrix of rows or columns
10   assigned to political parties or non-partisan candidates and
11   columns or rows assigned to offices and contests. The display
12   may consist of a contiguous matrix of the entire ballot or it may
13   be segmented to present portions of the ballot in succession.

14   45.5.2.3.11 The voting system shall provide a facility for the definition of
15   the ballot, including the definition of the number of allowable
16   choices for each office and contest, and for special voting
17   options such as write-in candidates. It shall provide for all
18   voting options and specifications as provided for in Articles 5
19   and 7, Title 1, C.R.S. The system shall generate all required
20   masters and distributed copies of the voting program in
21   conformance with the definition of the ballot for each voting
22   device and remote site. The distributed copies, resident or
23   installed in each voting device, shall include all software
24   modules required to: monitor system status and generate
25   machine-level audit reports, accommodate device control
26   functions performed by remote location officials and
27   maintenance personnel, and register and accumulate votes.

28   45.5.2.3.12 ~~All~~ THE TRUSTED BUILD OF THE voting system software,
29   installation programs, and third party software (such as
30   operating systems, drivers, etc.) used to install or to be installed
31   on voting system devices shall be distributed on a write-once
32   media.

33   45.5.2.3.13 The voting system shall allow the system ~~administrator~~
34   ADMINISTRATIVE ACCOUNT to verify that the software installed
35   is the certified software by comparing it to THE "TRUSTED
36   BUILD" OR OTHER reference information.

37   45.5.2.3.14 All DRE voting devices shall use touch screen technology or
38   other technology providing ~~accurate~~ visual ballot display and
39   selection.   The voting system provider shall include
40   documentation concerning the use of touch screen or other
41   display and selection technology, including but not limited to:

Formatted: Small caps

1   (a)   Technical documentation describing the nature and
2   sensitivity of the tactile device (if the system uses touch
3   screen technology);

4   (b)   Technical documentation describing the nature and
5   sensitivity of any other technology used to display and
6   select offices, candidates, or issues;

7   (c)   Any mean time between failure (MTBF) data collected on
8   the vote recording devices; and

9   (d)   Any available data on problems caused for persons who
10   experience epileptic seizures due to the DRE voting
11   devices' screen refresh rate. ~~FAILURE BY THE VOTING SYSTEM PROVIDER TO PROVIDE THIS~~
12   ~~DOCUMENTATION WITHIN THE TIMELINES ESTABLISHED IN~~
13   ~~SECTION 45.3.3 SHALL DELAY THE CERTIFICATION PROCESS~~

15   45.5.2.3.15   The voting system shall contain a control subsystem that
16   consists of the physical devices and software that accomplish
17   and validate the following operations.

18   (a)   Voting system Preparation - The control subsystem shall
19   encompass the hardware and software required to prepare
20   remote location voting devices and memory devices for
21   election use. Remote site preparation includes all
22   operations necessary to install ballot displays, software,
23   and memory devices in each voting device. The control
24   subsystem shall be designed in such a manner as to
25   facilitate the automated validation of ballot and software
26   installation and to detect errors arising from their incorrect
27   selection or improper installation.

28   (b)   Error Detection – the voting system shall contain a
29   detailed list and description of the error messages that will
30   appear on the voting devices, the controller (if any), the
31   paper ballot printer, programmer, or any other device used
32   in the voting process to indicate that a component has
33   failed or is malfunctioning.

34   45.5.2.3.16   The voting system shall have a high level of integration between
35   the ballot layout subsystem and the vote tabulation subsystem.
36   This integration shall permit and facilitate the automatic transfer
37   of all ballot setup information from the automated ballot layout
38   module to the single ballot tabulation system that will be used in
39   a fully integrated manner for DRE, optical scan, and any other
40   voting devices included in the voting system.

45.5.2.3.17   The processing subsystem contains all mechanical, electromechanical, and electronic devices required to perform the logical and numerical functions of interpreting the electronic image of the voted ballot and assigning votes to the proper memory registers. Attributes of the processing subsystem that affect its suitability for use in a voting system, are accuracy, speed, reliability, and maintainability.

   (a)   Processing accuracy refers to the ability of the subsystem to receive electronic signals produced by vote marks and timing information, to perform logical and numerical operations upon these data, and to reproduce the contents of memory when required without error. Processing subsystem accuracy shall be measured as bit error rate, which is the ratio of uncorrected data bit errors to the number of total data bits processed when the system is operated at its nominal or design rate of processing in a time interval of four (4) hours. The bit error rate shall include all errors from any source in the processing subsystem. For all types of systems, the Maximum Acceptable Value (MAV) for this error rate shall be one (1) part in five hundred thousand (500,000) ballot positions, and the Nominal Specification Value (NSV) shall be one (1) part in ten million (10,000,000) ballot positions.

   (b)   Memory devices that are used to retain control programs and data shall have demonstrated at least a ninety-nine and a half (99.5) percent probability of error-free data retention for a period of six months for operation and non-operation.

45.5.2.3.18   The reporting subsystem contains all mechanical, electromechanical, and electronic devices required to print reports of the tabulation. The subsystem also may include data storage media and communications devices for transportation or transmission of data to other sites. Communications Devices shall not be used for the preparation or printing of an official canvass of the vote unless they conform to a data interchange and interface structure and protocol that incorporates some form of error checking and auditing process control.

45.5.2.3.19   The approach to design shall be unrestricted, and it may incorporate any form or variant of technology that is capable of meeting the requirements of this rule, and other attributes specified herein. The frequency of voting system malfunctions and maintenance requirements shall be reduced to the lowest

level consistent with cost constraints. Applicants are required to use MIL-STD-454; "Standard General Requirements for Electronic Equipment" that is hereby adopted and incorporated by reference, as a guide in the selection and application of materials and parts.

45.5.2.3.20 ALL ELECTRICAL VOTING DEVICES PROVIDED 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 THREE HOURS THE ABILITY TO:

(I) CONTINUE TO SCAN OR IMAGE VOTERS' BALLOTS;

(II) TABULATE ACCURATELY VOTERS' CHOICES FROM THE BALLOTS,

(III) STORE ACCURATELY A VOTERS' BALLOT CHOICES DURING A PERIOD OF ELECTRICAL OUTAGE; AND

(IV) TRANSMIT REQUIRED RESULTS FILES ACCURATELY IF POWER FAILURE EXPERIENCED DURING TRANSMITTAL OF RESULTS.

(B) FOR DRE DEVICES, THIS CAPABILITY SHALL INCLUDE AT A MINIMUM FOR A PERIOD OF NOT LESS THAN 8 HOURS THE ABILITY TO:

(I) CONTINUE TO PRESENT BALLOT saccurately 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 EXPERIENCED DURING TRANSMITTAL OF RESULTS.

Formatted: Small caps

Formatted: Small caps

Formatted: Small caps

Formatted: Bullets and Numbering

(C) ——FOR V-VPAT DEVICES CONNECTED TO DRES, THIS CAPABILITY SHALL INCLUDE AT A MINIMUM FOR A PERIOD OF NOT LESS THAN 8 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 PROBLEMS.

(D)   THE VOTING SYSTEM PROVIDER SHALL DELIVER TO THE SOS DOCUMENTATION DETAILING ESTIMATED TIME OF OPERATION ON BATTERY 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 SOS DOCUMENTATION SPECIFYING THE STEPS AND TIMES REQUIRED FOR CHARGING BATTERIES FOR EACH TYPE OF OPTICAL SCANNER, BALLOT IMAGER, DRE AND V-VPAT THEY PROVIDE.

45.5.2.3.21   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 USER ACCOUNT IS CURRENTLY WORKING.

45.5.2.3.22   THE VOTING SYSTEM SHALL PROVIDE CAPABILITIES TO ENFORCE 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.

Formatted: Indent: First line: 0"

Formatted: Indent: Hanging: 0.88", Tab stops: 2.5", Left + Not at 1.63"

Formatted: Indent: Left: 1.63", First line: 0"

45.5.2.3.23̶0̶ The voting system and all associated components shall have a̶ AN ESTIMATED useful life of at least eight (8) years. VOTING SYSTEM PROVIDER SHALL PROVIDE DOCUMENTATION OF BASIS FOR THE ESTIMATE.

45.5.2.3.24̶1̶ The voting system provider shall submit drawings, photographs, and any related brochure documents to assist with the evaluation of the physical design of the use of the voting system.

45.5.2.4 Documentation Requirements

45.5.2.4.1 In addition to Section 45.3 above, 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 materials)

(D)• Systems Programming and Diagnostics Manuals

(E) A LIST OF MINIMUM SERVICES NEEDED FOR SUCCESSFUL, SECURE AND HARDENED OPERATION OF ALL COMPONENTS OF VOTING SYSTEM.

45.5.2.4.2 All ITA qualification reports t̶h̶a̶t̶ ̶a̶r̶e̶ ̶m̶a̶t̶e̶r̶i̶a̶l̶ ̶t̶o̶ ̶t̶h̶e̶ ̶d̶e̶t̶e̶r̶m̶i̶n̶a̶t̶i̶o̶n̶ ̶t̶h̶a̶t̶ ̶a̶ ̶v̶o̶t̶i̶n̶g̶ ̶s̶y̶s̶t̶e̶m̶ ̶m̶a̶y̶ ̶b̶e̶ ̶c̶e̶r̶t̶i̶f̶i̶e̶d̶ shall be evaluated to determine if the test procedures, records of testing, and reporting of results meet the requirements of this rule AND THE APPLICABLE FEDERAL CERTIFICATION REQUIREMENTS AT THE TIME OF CERTIFICATION.

45.5.2.4.3 PRIOR TO APPLYING FOR CERTIFICATION, THE VOTING SYSTEM PROVIDER SHALL HAVE COMPLETED AN INDEPENDENT ANALYSIS OF THE SYSTEM WHICH INCLUDES:

(A) APPLICATION PENETRATION TEST CONDUCTED TO OSSTMM 2.2 STANDARDS FOR WHITE OR DOUBLE GRAY BOX TESTING; [̶A̶D̶D̶I̶T̶I̶O̶N̶A̶L̶ ̶D̶E̶T̶A̶I̶L̶S̶ ̶T̶O̶ ̶B̶E̶ ̶D̶E̶V̶E̶L̶O̶P̶E̶D̶]̶

(B) SOURCE CODE EVALUATION TO THE COMMON CRITERIA CERTIFICATION AT EVALUATION ASSURANCE LEVEL 4 (EAL-4) FOR SOFTWARE SECURITY WEAKNESSES; [̶A̶D̶D̶I̶T̶I̶O̶N̶A̶L̶ ̶D̶E̶T̶A̶I̶L̶S̶ ̶T̶O̶ ̶B̶E̶ ̶D̶E̶V̶E̶L̶O̶P̶E̶D̶]̶

(C~~D~~) A LIST OF APPROVED CONTRACTORS WILL BE PROVIDED UPON REQUEST OF THE VOTING SYSTEM PROVIDER TO PERFORM THE INDEPENDENT ANALYSIS.~~; [ADDITIONAL DETAILS TO BE DEVELOPED]~~

~~(C)   [ADDITIONAL CRITERIA TO BE DEVELOPED]~~

45.5.2.4.~~3~~4   Documentation submitted to the SOS shall be reviewed to ensure the voting system meets the 2002 VOTING SYSTEMS STANDARDS, OR THE MOST CURRENT, IMPLEMENTED VOTING SYSTEM STANDARDS ENACTED BY THE EAC. ~~FEC. The submitted documentation shall include methods for implementing future releases and versions of the future standards.~~

(A)   VENDORS SHALL PROVIDE THE SOS WITH THEIR DOCUMENTED PROJECT PLANS FOR MODIFYING THEIR VOTING SYSTEMS TO COMPLY WITH AND ACHIEVE CERTIFICATION UNDER THE EAC'S ADOPTED 2005 VOLUNTARY VOTING SYSTEM GUIDELINES BY JANUARY 1, 2008 IF NOT CURRENTLY TESTED AND CERTIFIED TO THAT STANDARD AT TIME OF APPLYING FOR CERTIFICATION.

45.5.2.4.5   FAILURE BY THE VOTING SYSTEM PROVIDER TO PROVIDE ANY DOCUMENTATION WITHIN THE TIMELINES ESTABLISHED IN THIS RULE SHALL DELAY THE CERTIFICATION PROCESS FOR THE SPECIFIC APPLICATION.

45.5.2.5 Audit capacity

45.5.2.5.1   The voting system shall be capable of producing ELECTRONIC AND PRINTED ~~paper~~ audit logs OF SYSTEM OPERATION AND SYSTEM OPERATORS WHICH SHALL BE SUFFICIENT TO ALLOW ALL OPERATIONS AND INPUT COMMANDS TO BE AUDITED ~~("Audits", "audit reports", or "audit records"), generated by the system components, or in some cases, by the system operators, from which all operations may be audited. Except for the storage of vote images that shall be maintained in a random sequence, the audit records shall be created and maintained in the sequence in which the operations were performed.~~

45.5.2.5.2   The voting system~~s~~ 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

(D)   ELECTION RESULT CONSOLIDATION AND REPORTING

45.5.2.5.3   The system shall track and maintain audit information of the following events:

(a)   Log on and log off activity

(b)   Application start and stop

(c)   Printing activity (where applicable)

(d)   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), and voting activity.

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

45.5.2.5.4   All tabulation devices shall display the unit serial number(s) both physically and within any applicable software or PROM/ROM devices.

45.5.2.5.5   If a vote tabulation device employs the use of removable memory storage devices, the devices shall allow for the transfer of audit records if the device and/or memory storage device is damaged or destroyed.

45.5.2.5.6   ALL TRANSACTION AUDIT RECORDS OF THE DATABASE SHALL BE MAINTAINED IN A FILE OUTSIDE OR SEPARATE FROM THE DATABASE. [CRITERIA TO BE DEVELOPED] WHICH IS NOT ACCESSIBLE BY USER ACCOUNTS.

45.5.2.6 Security Requirements

45.5.2.6.1   ALL VOTING SYSTEMS SUBMITTED FOR CERTIFICATION SHALL MEET THE FOLLOWING MINIMUM SYSTEM SECURITY REQUIREMENTS:

(A)   THE VOTING SYSTEM SHALL ACCOMMODATE A GENERAL SYSTEM OF ACCESS BY LEAST PRIVILEGE OR AND ROLE

BASED ACCESS CONTROL. THE FOLLOWING REQUIREMENTS SHALL APPLY:

(I) ~~ADMINISTRATOR~~ ADMINISTRATIVE SYSTEM ACCOUNT ~~OF SYSTEM~~ DOES NOT HAVE ACCESS TO ADMINISTRATIVE RIGHTS TO THE DATABASE AND DOES NOT HAVE THE ABILITY OR KNOWLEDGE OF THE DATABASE ADMINISTRATOR PASSWORD;

(II) A UNIQUE SYSTEM USER ACCOUNT SHALL BE CREATED FOR OPERATING SYSTEM USE THAT IS 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.

(D) NO ACCESS TO MODIFY OTHER USER ACCOUNTS ON THE SYSTEM.

(III) A UNIQUE APPLICATION ADMINISTRATIVE ACCOUNT SHALL BE CREATED WHICH HAS FULL ACCESS AND RIGHTS TO THE APPLICATION AND DATABASE.

~~ADMINISTRATOR OF APPLICATION; [CRITERIA TO BE DEVELOPED]~~

(IV) A UNIQUE APPLICATION USER ACCOUNT SHALL BE CREATED WITH LIMITED RIGHTS SPECIFICALLY DESIGNE TO PERFORM FUNCTIONAL OPERATION WITHIN THE SCOPE OF THE APPLICATION. THIS USER SHALL BE RESTRICTED IN THE CREATION OR MODIFICATION OF ANY USER ACCOUNTS.

~~ADMINISTRATOR OF DATABASE; [CRITERIA TO BE DEVELOPED]~~

(V) VOTING SYSTEM PROVIDER SHALL NOT HAVE ADMINISTRATIVE ACOCUNT, OR ADMINISTRATIVE ACCOUNT ACCESS.

Formatted: Bullets and Numbering

Formatted: Numbered + Level: 1 + Numbering Style: A, B, C, … + Start at: 1 + Alignment: Left + Aligned at: 3.5" + Tab after: 4" + Indent at: 4"

Formatted: Indent: Left: 2.88", Hanging: 0.63", Tab stops: 3.5", Left + Not at 2.88"

Formatted: Bullets and Numbering

(B)   THE VOTING SYSTEM SHALL MEET THE FOLLOWING
       REQUIREMENTS FOR NETWORK SECURITY:

       (I)   ALL COMPONENTS OF THE VOTING SYSTEM SHALL
              ONLY BE OPERATED ON A CLOSED NETWORK ONLY
              FOR THE USE OF THE VOTING SYSTEM;

       (II)   VENDOR DOCUMENTATION 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;

       (III) THE VOTING SYSTEM SHALL BE TESTED TO
              CONTAIN PROVISIONS FOR UPDATING SECURITY
              PATCHES, SOFTWARE AND/OR SERVICE PACKS
              WITHOUT ACCESS TO THE OPEN NETWORK.

              [ADDITIONAL REQUIREMENTS TO BE DEVELOPED]

(C)   THE VOTING SYSTEM SHALL MEET THE FOLLOWING
       REQUIREMENTS FOR DATABASE SECURITY:

       (I)   AFTER JANUARY 1 MARCH 31, 2008 ALL VOTING
              SYSTEM DATABASE DESIGNS MUST BE HARDENED TO
              THE FOLLOWING MINIMUM THE REQUIREMENTS
              IDENTIFIED IN THE NSA GUIDELINES FOR DATABASE
              HARDENING:

              1. DATABASE AUTHENTICATION FOR WINDOWS
                  BASED OPERATING SYSTEMS SHALL USE WINDOWS
                  AUTHENTICATION MODE;

              2. THE "GUEST" USER ACCOUNT SHALL BE DELETED
                  FROM ALL OPERATING SYSTEMS AND DATABASE
                  ACCESS;

              3. STATEMENT PERMISSIONS ARE NOT GRANTED TO
                  ANY USER LEVEL ACCOUNT OF THE VOTING SYSTEM

              4. STORED PROCEDURES SHALL BE EXECUTED USING
                  ONLY ADO COMMANDS.

              5. THE FOLLOWING LIST OF STORED PROCEDURES
                  SHALL BE DISABLED BY DENYING EXECUTE

Formatted: Indent: Left: 2.88", Hanging: 0.38", Tab stops: -2.63", Left + 0", Left + 0.25", Left + 3.25", Left + Not at 0.5" + 1" + 1.25" + 2.5" + 2.88"

1
2 PERMISSIONS FOR ALL DATABASE USERS AND ANY
APPLICATION ON THE HOST COMPUTER:

3 SP_OACREATE

4 SP_OASTOP

5 SP_OADESTROY

6 SP_OASETPROPERTY

7 XP_REGADDMULTISTRING

8 XP_REGDELETEKEY

9 XP_REGDELETEVALUE

10 XP_REGENUMVALUES

11 XP_REGREMOVEMULTISTRING

12 SP_BINDSESSION

13 SP_CURSOR

14 SP_CURSORCLOSE

15 SP_CURSORFETCH

16 SP_CURSOROPEN

17 SP_CURSOROPTION

18 SP_GETBINDTOKEN

19 SP_GETMBCSCHARLEN

20 SP_ISMBCSLEADBYTE

21 SP_REPLCMDS

22 SP_REPLCOUNTERS

23 SP_REPLDONE

24 SP_REPLFLUSH

25 SP_REPLSTATUS

26 SP_REPLTRANS

1   SP_SDIDEBUG

2   XP_AVAILABLEMEDIA

3   XP_CMDSHELL

4   XP_DELETEMAIL

5   XP_DIRTREE

6   XP_DROPWEBTASK

7   XP_DSNINFO

8   XP_ENUMDSN

9   XP_ENUMERRORLOGS

10   XP_ENUMGROUPS

11   XP_ENUMQUEUEDTASKS

12   XP_EVENTLOG

13   XP_FINDNEXTMSG

14   XP_FIXEDDRIVES

15   XP_GETFILEDETAILS

16   XP_GETNETNAME

17   XP_GRANTLOGIN

18   XP_LOGEVENT

19   XP_LOGINCONFIG

20   XP_LOGININFO

21   XP_MAKEWEBTASK

22   XP_MSVER

23   XP_PERFEND

24   XP_PERFMONITOR

25   XP_PERFSAMPLE

XP_PERFSTART

XP_READERRORLOG

XP_READMAIL

XP_REVOKELOGIN

XP_RUNWEBTASK

XP_SCHEDULERSIGNAL

XP_SENDMAIL

XP_SERVICECONTROL

XP_SNMP_GETSTATE

XP_SNMP_RAISETRAP

XP_SPRINTF

XP_SQLINVENTORY

XP_SQLREGISTER

XP_SQLTRACE

XP_SSCANF

XP-STARTMAIL

XP_STOPMAIL

XP_SUBDIRS

XP_UNC_TO_DRIVE;

; [ADDITIONAL CRITERIA TO BE DEVELOPED]

(II)• AFTER JANUARY 1MARCH 31, 2008. ALL VOTING
SYSTEMS DATABASES MUST BE RESTRICTED TO
ALLOWING ACCESS TO DATABASE AUTHENTICATION
FROM APPLICATION ONLY; (OR THROUGH
APPLICATION ONLY);.

(III)• ALL DATA STORED AT REST IN ANY VOTING SYSTEM
DATABASE SHALL BE ENCRYPTED TO 128 BIT DES;
[ADDITIONAL CRITERIA TO BE DEVELOPED]IN

Formatted: Indent: Left: 3.25", Hanging: 0.38", Tab stops: -2.63", Left + 0", Left + 0.25", Left + 1.5", Left + 3.63", Left + Not at 1.25" + 2.5" + 2.88"

ACCORDANCE WITH SECTION (V) OF THIS
REQUIREMENT;

(IV) ODBC CONNECTIONS ARE PROHIBITED FOR THE
VOTING SYSTEM SOFTWARE. ALL OPERATING SYSTEM
SERVICES RELATED TO THE USE OF THIS FEATURE
SHALL BE DISABLED; [ADDITIONAL CRITERIA TO BE
DEVELOPED]

DATA ENCRYPTION STANDARDS AND DATA
ENCRYPTION USAGE - DEFINING THE ALGORITHM FOR
ENCRYPTION; [ADDITIONAL CRITERIA TO BE
DEVELOPED]

(V) ALL CRYPTOGRAPHY MODULES SHALL BE
DOCUMENTED BY THE VOTING SYSTEM VENDOR TO BE
IN COMPLIANCE WITH CERTIFIED TO US FEDERAL
INFORMATION PROCESSING STANDARD (FIPS-140-2),
AND VALIDATED TO FIPS 180 STANDARDS.
[ADDITIONAL CRITERIA TO BE DEVELOPED]

(D)   THE VOTING SYSTEM SHALL MEET THE FOLLOWING
REQUIREMENTS FOR OPERATING SYSTEM SECURITY:

(I)   THE HOST COMPUTER OPERATING SYSTEM MAY
USE ANY OR ALL OF THE FOLLOWING ACCEPTABLE
SERVICES:

1.   ALERTER;

2.   APPLICATION MANAGEMENT;

3.   EVENT LOG;

4.   INDEXING SERVICE;

5.   LICENSE LOGGING SERVICE;

6.   LOGICAL DISK MANAGER;

7.   LOGICAL DISK MANAGER
ADMINISTRATIVE SERVICES;

8.   PERFORMANCE LOGS AND ALERTS;

9.   PLUG AND PLAY;

Formatted: Indent: Left: 0.88", Hanging: 3.13", Tab stops: 3.5", Left + 4", Left + Not at 1.25" + 2.5" + 2.88"

10. PRINT SPOOLER;

11. PROTECTED STORAGE;

12. REMOTE PROCEDURE CALL;

13. REMOVABLE STORAGE;

14. SECURITY ACCOUNTS MANAGER;

15. SIMPLE TCP/IP SERVICES;

16. SMART CARD;

17. SMART CARD HELPER;

18. SYSTEM EVENT NOTIFICATION;

19. UNINTERRUPTIBLE POWER SUPPLY;

20. WINDOWS MANAGEMENT INSTRUMENTATION;

21. WINDOWS MEDIA PROGRAM SERVICE;

22. WINDOWS MEDIA STATION SERVICE;

23. WINDOWS TIME SERVICE; AND

24. WORKSTATION.

(I) THE VOTING SYSTEM SHALL BE FULLY FUNCTIONAL WITH THE FOLLOWING SERVICES DISABLED (NOT TO BE TURNED ON EVEN MANUALLY) BY THE OPERATING SYSTEM:

1. ODBC;

2. MESSENGER;

3. AUTOMATIC UPDATES;

4. DNS CLIENT;

5. NETMEETING remote desktop sharing;

6IV.   BACKGROUND INTELLIGENT TRANSFER SERVICES;

7.   CLIPBOOK;

8.   FAX SERVICES;

9.   FTP PUBLISHING;

10.   NET LOGON;

11.   REMOTE DESKTOP HELP SESSION MANAGER;

12.   REMOTE REGISTRY SERVICE;

13.   SIMPLE MAIL TRANSFER PROTOCOL;

14.   SIMPLE NETWORK MANAGEMENT PROTOCOL;

15.   TELNET; AND

16.   WORLD WIDE WEB PUBLISHING SERVICES.

[ADDITIONAL SERVICES THAT MUST BE DISABLED TO BE DEVELOPED].

(II)   THE VOTING SYSTEM SHALL BE FULLY FUNCTIONAL WITH THE FOLLOWING SERVICES DISABLED UNTIL THE ELECTION MANAGEMENT SOFTWARE TRUSTED ROLE/USER ENABLES THE SERVICE. THESE SERVICES MUST BE DISABLED BY THE TRUSTED ROLUE/USER WHEN THE SERVICE IS NO LONGER REQUIRED FOR PROGRAM EXECUTION:

1.   ALERTER;

2.   COMPUTER BROWSER;

3.   IIS ADMIN SERVICE;

4.   ROUTING AND REMOTE ACCESS;

5.   TASK SCHEDULER; AND

6.   UNIVERSAL DEVICE PLUG AND PLAY HOST.

- THE VOTING SYSTEM SHALL BE FULLY FUNCTIONAL WITH THE FOLLOWING LIST OF PROHIBITED APPLICATIONS:

    I.   ANY/ALL IRQ/IM APPLICATIONS;

    II.   [ADDITIONAL APPLICATIONS THAT ARE PROHIBITED TO BE DEVELOPED].

(III) THE VOTING SYSTEM PROVIDER SHALL PROVIDE DOCUMENTATION CONTAINING A LIST OF MINIMUM SERVICES AND EXECUTABLES THAT ARE REQUIRED TO RUN THE VOTING SYSTEM APPLICATION.

(IV) THE VOTING SYSTEM PROVIDER SHALL DISABLE AUTO BOOT AND AUTO RUN FEATURES CAPABLE BY OPERATING SYSTEM. AUTO RUN MEANS FOR THE SYSTEM TO TAKE AN ACTION UPON THE INSERTING A REMOVABLE MEDIA. AUTO BOOT MEANS

(V) THE VOTING SYSTEM PROVIDER SHALL USE A VIRUS PROTECTION/PREVENTION APPLICATION ON THE ELECTION MANAGEMENT SERVER(S) /WORKSTATIONS WHICH MUST BE CAPABLE OF MANUAL UPDATES WITHOUT THE USE OF THE INTERNET.

- [ADDITIONAL REQUIREMENTS TO BE DEVELOPED]

(E) THE VOTING SYSTEM SHALL MEET THE FOLLOWING REQUIREMENTS FOR PASSWORD SECURITY:

(I) ALL PASSWORDS SHALL BE STORED AND USED IN A NON-REVERSIBLE ENCRYPTED/HARD-CODED FORMAT;

(II) PASSWORDS TO DATABASE MUST NOT BE STORED IN DATABASE; [ADDITIONAL CRITERIA TO BE DEVELOPED]

(III) PASSWORD TO DATABASE SHALL BE OWNED AND ONLY KNOWN BY APPLICATION;

(III)(IV) THE APPLICATION'S DATABASE MANAGEMENT SYSTEM SHALL REQUIRE SEPARATE PASSWORDS FOR

Formatted: Bullets and Numbering

THE ADMINISTRATIVE AND EACH USER ACCOUNT
WITH ACCESS TO THE APPLICATION.

(V) THE SYSTEM SHALL BE DESIGNED IN SUCH A WAY
THAT THE USE OF THE ADMINISTRAT~~OR~~IVE
ACCOUT PASSWORD SHALL NOT BE REQUIRED FOR
NORMAL OPERATING FUNCTIONS AT ANY REMOTE
LOCATION.

(VI) THE SYSTEM SHALL BE DESIGNED UN SUCH A WAY
TO FACILITATE THE CHANGING OF PASSWORDS
FOR EACH ELECTION CYCLE.

(VII) 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.

(VIII) BY MARCH 31, 2008 ALL COMPONENTS OF
VOTING SYSTEM SHALL BE CAPABLE OF
SUPPORTING PASSWORDS OF A MINIMUM OF 8
CHARACTERS, WHICH 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 SHALL BE IN COMPLIANCE
WITH KNOWN SOFTWARE CODING STANDARDS APPLICABLE
TO THE BASE LANGUAGE OF THE APPLICATION. THE VOTING
SYSTEM SHALL MEET THE FOLLOWING MINIMUM
REQUIREMENTS FOR SOFTWARE SECURITY:

~~ALL VOTING SYSTEM SOFTWARE SHALL BE IN~~
~~COMPLIANCE WITH KNOWN SOFTWARE CODING~~
~~STANDARDS APPLICABLE TO THE BASE LANGUAGE~~
~~OF THE APPLICATION MEETING THE FOLLOWING~~
~~MINIMUM STANDARDS: [TO BE DEVELOPED]~~

(I) SOFTWARE SHALL BE VALIDATED TO THE
COMMON CRITERIA CERTIFICATION AT
EVALUATION ASSURANCE LEVEL 4 (EAL-4) FOR
SOFTWARE SECURITY WEAKNESSES;

(II) USE OF HIGH LEVEL PROGRAMMING LANGUAGES
SHALL BE LIMITED TO: PASCAL, VISUAL BASIC
6.0 OR LATER, JAVA, C, C++, AND C#. THE
REQUIREMENT FOR THE USE OF HIGH-LEVEL

LANGUAGE FOR LOGICAL OPERATIONS DOES NOT PRECLUDE THE USE OF ASSEMBLY LANGUAGE FOR HARDWARE-RELATED SEGMENTS, SUCH AS DEVICE CONTROLLERS AND HANDLER PROGRAMS.

[Comment: Rather than limiting the languages in this section, consider adopting the language in section 5.2 if the 2005 VVSG:

5.2.1 Selection of Programming Languages

Software associated with the logical and numerical operations of vote data shall use a highlevel programming language, such as: Pascal, Visual Basic, Java, C and C++. The requirement for the use of high-level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.]

(III)   THE FOLLOWING INPUT VALIDATIONS SHALL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1. PATH MANIPULATION;

2. CROSS SITE SCRIPTING.BASIC X;

3. RESOURCE INJECTION;

4. OS COMMAND INJECTION (ALSO CALLED "SHELL INJECTION");

5. SQL INJECTION.

(IV)   THE FOLLOWING RANGE ERRORS SHALL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1. STACK OVERFLOW;

2. HEAP OVERFLOW;

3. FORMAT STRING VULNERABILITY;

4. IMPROPER NULL TERMINATION.

(V) THE FOLLOWING API ABUSES WILL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1. HEAP INSPECTION;

2. STRING MANAGEMENT/MANIPULATION.

(VI) THE FOLLOWING TIME AND STATE CONDITIONS SHALL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1. TIME-OF-CHECK/TIME-OF-USE RACE CONDITION;

2. UNCHECKED ERROR CONDITION.

(VII) THE FOLLOWING CODE QUALITY CONDITIONS SHALL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1. MEMORY LEAKS;

2. UNRESTRICTED CRITICAL RESOURCE LOCK;

3. DOUBLE FREE;

4. USE AFTER FREE;

5. UNINTIALIZED VARIABLE;

6. UNINTENTIONAL POINTER SCALING;

7. IMPROPER POINTER SUBTRACTION;

8. NULL DEREFERENCE.

(VII) THE FOLLOWING ENCAPSULATION CONDITIONS SHALL BE PROHIBITED AND VERIFIED THROUGH INDEPENDENT ANALYSIS IN ACCORDANCE WITH

SECTION 45.5.2.4.3: [ADDITIONAL CRITERIA TO BE DEVELOPED]

1ɪ.   PRIVATE ARRAY-TYPED FIELD RETURNED FROM A PUBLIC METHOD;

2ɪɪ.   PUBLIC DATA ASSIGNED TO PRIVATE ARRAY-TYPED FIELD;

3ɪɪɪ.   OVERFLOW OF STATIC INTERNAL BUFFER;

4ɪᴠ.   LEFTOVER DEBUG CODE.

[Comment: For sub-sections F(III) through F(VII)of rule 45.5.2.6.1, consider adopting a modifies version of the provisions of the 2005 VVSG listed below. Modifying these sections to meet Colorado statutory requirements might provide clear and reasonably testable guidelines.

5.2 Software Design and Coding Standards

The software used by voting systems is selected by the vendor and not prescribed by the Guidelines. This section provides requirements for voting system software with regard to:
- Selection of programming languages
- Software integrity
- Software modularity and programming
- Control constructs
- Naming conventions
- Coding conventions
- Comment conventions

5.2.1 Selection of Programming Languages

Software associated with the logical and numerical operations of vote data shall use a highlevel programming language, such as: Pascal, Visual Basic, Java, C and C++. The requirement for the use of high-level language for logical operations does not preclude the use of assembly language for hardware-related segments, such as device controllers and handler programs. Also, operating system software may be designed in assembly language.

5.2.2 Software Integrity

Self-modifying, dynamically loaded or interpreted code is prohibited, except under the security provisions outlined in Subsection 7.4. This prohibition is to ensure that the software tested and approved during the certification process remains unchanged and retains its integrity. External modification of code during execution shall be prohibited. Where the development environment (programming language and development tools) includes the following features, the software shall provide controls to prevent accidental or deliberate attempts to replace executable code:
- a. Unbounded arrays or strings (includes buffers used to move data)
- b. Pointer variables
- c. Dynamic memory allocation and management

5.2.3 Software Modularity and Programming

Voting system application software, including commercial off-the-shelf (COTS) software, shall be designed in a modular fashion. However, COTS software is not required to be

inspected for compliance with this requirement. For the purpose of this requirement, "modules" may be compiled or interpreted independently. Modules may also be nested. The modularity rules described here apply to the component sub-modules of a library. The principle to be followed is that the module contains all the elements to compile or interpret successfully and has limited access to data in other modules. The design concept is simple replacement with another module whose interfaces match the original module. A module is designed in accordance with the rules below.

a. Each module shall have a specific function that can be tested and verified independently of the remainder of the code. In practice, some additional modules (such as library modules) may be needed to compile the module under test, but the modular construction allows the supporting modules to be replaced by special test versions that support test objectives.

b. Each module shall be uniquely and mnemonically named, using names that differ by more than a single character. In addition to the unique name, the modules shall include a set of header comments identifying the module's purpose, design, conditions, and version history, followed by the operational code. Headers are optional for modules of fewer than ten executable lines where the subject module is embedded in a larger module that has a header containing the header information. Library modules shall also have a header comment describing the purpose of the library and version information.

c. All required resources, such as data accessed by the module, should either be contained within the module or explicitly identified as input or output to the module. Within the constraints of the programming language, such resources shall be placed at the lowest level where shared access is needed. If that shared access level is across multiple modules, the definitions should be defined in a single file (called header files in some languages, such as C) where any changes can be applied once and the change automatically applies to all modules upon compilation or activation.

d. A module is small enough to be easy to follow and understand. Program logic visible on a single page is easy to follow and correct. Volume II, Section 5 provides testing guidelines for the accredited test lab to identify large modules subject to review under this requirement.

e. Each module shall have a single entry point, and a single exit point, for normal process flow. For library modules or languages such as the object-oriented languages, the entry point is to the individual contained module or method invoked. The single exit point is the point where control is returned. At that point, the data that is expected as output must be appropriately set. The exception for the exit point is where a problem is so severe that execution cannot be resumed. In this case, the design must explicitly protect all recorded votes and audit log information and must implement formal exception handlers provided by the language.

f. Process flow within the modules shall be restricted to combinations of the control structures defined in Volume II, Section 5. These structures support the modular concept, especially the single entry and exit rule above. They apply to any language feature where program control passes from one activity to the next, such as control scripts, object methods or sets of executable statements, even though the language itself is not procedural

5.2.4 Control Constructs

Voting system software shall use the control constructs identified in Volume II, Section 5:

    a. Acceptable constructs are Sequence, If-Then-Else, Do-While, Do-Until, Case, and the General Loop (including the special case for loop).

        i. If the programming language used does not provide these control constructs, the vendor shall provide comparable control structure logic. The constructs shall be used consistently throughout the code. No other constructs shall be used to control program logic and execution.

        ii. While some programming languages do not create programs as linear processes, stepping from an initial condition through changes to a conclusion, the program components nonetheless contain procedures (such as "methods" in object-oriented languages). Even in these programming languages, the procedures must execute through these control constructs or their equivalents, as defined and provided by the vendor.

        iii. Operator intervention or logic that evaluates received or stored data shall not redirect program control within a program routine. Program control may be redirected within a routine by calling subroutines, procedures, and functions, and by interrupt service routines and exception handlers (due to abnormal error conditions). Do-While (False) constructs and intentional exceptions (used as GoTos) are prohibited.

5.2.5 Naming Conventions

Voting system software shall use the naming conventions below.

    a. Object, function, procedure, and variable names shall be chosen to enhance the readability and intelligibility of the program. Insofar as possible, names shall be selected so that their parts of speech represent their use, such as nouns to represent objects and verbs to represent functions.

    b. Names used in code and in documentation shall be consistent.

    c. Names shall be unique within an application. Names shall differ by more than a single character. All single-character names are forbidden except those for variables used as loop indexes. In large systems where subsystems tend to be developed independently, duplicate names may be used where the scope of the name is unique within the application. Names should always be unique where modules are shared.

    d. Language keywords shall not be used as names of objects, functions, procedures, variables or in any manner not consistent with the design of the language.

5.2.6 Coding Conventions

Voting system software shall adhere to basic coding conventions. The coding conventions used shall meet one of the following conditions:

    a. The vendors shall identify the published, reviewed, and industry-accepted coding conventions used and the accredited test lab shall test for compliance

    b. The accredited test lab shall evaluate the code using the coding convention requirements specified in Volume II, Section 5 These guidelines reference conventions that protect the integrity and security of the code, which may be language-specific and language-independent conventions that significantly contribute to readability and maintainability. Specific style conventions that support economical testing are not binding unless adopted by the vendor.

5.2.7 Comment Conventions

Voting system software shall use the following comment conventions:

a. All modules shall contain headers. For small modules of 10 lines or less, the header may be limited to identification of unit and revision information. Other header information should be included in the small unit headers if not clear from the actual lines of code. Header comments shall provide the following information:

    i. The purpose of the unit and how it works

    ii. Other units called and the calling sequence

    iii. A description of input parameters and outputs

    iv. File references by name and method of access (i.e., read, write, modify or append)

    v. Global variables used

    vi. Date of creation and a revision record

b. Descriptive comments shall be provided to identify objects and data types. All variables shall have comments at the point of declaration clearly explaining their use. Where multiple variables that share the same meaning are required, the variables may share the same comment

c. In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching d. Assembly code shall contain descriptive and informative comments such that its executable lines can be clearly understood

e. All comments shall be formatted in a uniform manner that makes it easy to distinguish them from executable code

7.4.1 Software and Firmware Installation

The system shall meet the following requirements for installation of software, including hardware with embedded firmware.

a. If software is resident in the system as firmware, the vendor shall require and state in the system documentation that every device is to be retested to validate each ROM prior to the start of elections operations.

b. To prevent alteration of executable code, no software shall be permanently installed or resident in the voting system unless the system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

c. 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.

d. 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.

e. After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.

7.4.2 Protection Against Malicious Software

Voting systems shall deploy protection against the many forms of threats to which they may be exposed such as file and macro viruses, worms, Trojan horses, and logic bombs. Vendors shall develop and document the procedures to be followed to ensure that such protection is maintained in a current status.

7.5.2 Protection Against External Threats
        a. Voting systems that use public telecommunications networks shall implement
        protections against external threats to which commercial products used in the system
        may be susceptible.
        b. 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.
                i. Such documentation shall identify the name, vendor, and version used for
                each such component.
        c. Voting systems that use public telecommunications networks shall use protective
        software at the receiving-end of all communications paths to:
                i. Detect the presence of a threat in a transmission
                ii. Remove the threat from infected files/data
                iii. Prevent against storage of the threat anywhere on the receiving device
                iv. Provide the capability to confirm that no threats are stored in system
                memory and in connected storage media
                v. Provide data to the system audit log indicating the detection of a threat and
                the processing performed
        d. Vendors shall use multiple forms of protective software as needed to provide
        capabilities for the full range of products used by the voting system.

7.5.3 Monitoring and Responding to External Threats
Voting systems that use public telecommunications networks may become vulnerable, by
virtue of their system components, to external threats to the accuracy and integrity of vote
recording, vote counting, and vote consolidation and reporting processes. Therefore, vendors
of such systems 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 vendor will use to:
        a. Monitor threats, such as through the review of assessments, advisories, and alerts for
        COTS components issued by the Computer Emergency Response Team (CERT), for
        which a current listing can be found at http://www.cert.org, the National Infrastructure
        Protection Center (NIPC), and the Federal Computer Incident Response Capability
        (FedCIRC), for which additional information can be found at www.uscert.gov
        b. Evaluate the threats and, if any, proposed responses
        c. Develop responsive updates to the system and/or corrective procedures
        d. Submit the proposed response to the test labs and appropriate states for approval,
        identifying the exact changes and whether or not they are temporary or permanent e.
        After implementation of the proposed response is approved by the state, assist clients,
        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
        state
        f. Address threats emerging too late to correct the system by:
                i. Providing prompt, emergency notification to the accredited test labs and the
                affected states and user jurisdictions

ii. Assisting client jurisdictions directly or advising them through detailed written procedures to disable the public telecommunications mode of the system
iii. Modifying the system after the election to address the threat, submitting the modified system to an accredited test lab and the EAC or state certification authority for approval, and assisting client jurisdictions directly or advising them through detailed written procedures, to update their systems and/or to implement the corrective procedures after approval]

(VIII)   THE APPLICATION SHALL NOT OPEN DATABASE TABLES FOR DIRECT EDITING.

(G)   AS OF MARCH 31 2008, THE VOTING SYSTEM SHALL MEET THE FOLLOWING MINIMUM REQUIREMENTS FOR REMOVABALE STORAGE MEDIA WITH DATA CONTROLS:

(I)   ALL DATA STORED SHALL BE AUTHENTICATED, ENCRYPTED, AND VALIDATED IN ACCORDANCE WITH CRYPTOGRAPHY REQUIREMENTS OF SUBSECTION (C)(V) OF THIS REQUIREMENT;

(II)   ANTIVIRUS SOFTWARE MUST SCAN REMOVABLE MEDIA UPON INSERTION OF MEDIA OR MEDIA DEVICE INTO HOST COMPUTER.

45.5.2.6.12 The voting system provider shall provide documentation detailing voting system security in the areas listed below. At no time shall THE SYSTEM SHALL CONTAIN DOCUMENTED CONFIGURATIONS, PROPERTIES AND PROCEDURES TO PREVENT, DETECT AND LOG a system allow for unauthorized 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)   Alteration 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.

45.5.2.6.2~~3~~   The voting system provider shall submit to the SOS 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)   WHAT SOFTWARE FOR VIRUS AND SPYWARE PROTECTION THE VOTING SYSTEM SHALL USE

(~~f~~G) General characteristics of supervisory access privileges;

(~~g~~H) Segregation of duties; and

(~~f~~I)   Any additional relevant characteristics.

45.5.2.6.3~~4~~   The voting system shall include detailed documentation as to 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 end users that purchase the voting system.

45.5.2.7 Telecommunications Requirements

45.5.2.7.1   Telecommunications includes all components of the ~~voting~~ system that transmit data over public or private ~~network~~ communications. ~~This includes wired, wireless, phone/ modem, LAN, and WAN connections.~~

45.5.2.7.2 ALL ELECTRONIC TRANSMISSIONS FROM A VOTING SYSTEM
~~ACROSS PUBLIC NETWORKS~~ SHALL MEET THE FOLLOWING
MINIMUM STANDARDS:

(A) MODEMS FROM REMOTE DEVICES SHALL BE "DIAL ONLY"
AND CANNOT BE PROGRAMMED TO RECEIVE A CALL;
~~[ADDITIONAL CRITERIA TO BE DEVELOPED]~~

(B) MODEMS FROM TALLY COMPUTER (CENTRAL SERVERS,
INCLUDING RALLY SERVERS) SHALL BE HARDENED TO
INDUSTRY STANDARDS WITH AUTHENTICATION;
~~[ADDITIONAL CRITERIA TO BE DEVELOPED]~~

(C) ALL COMMUNICATIONS OF DATA IN TRANSFER SHALL BE
ENCRYPTED, AUTHENTICATED AND AUTHORIZED TO THE
FIPS 140-2 STANDARD AND VERIFIED TO THE FIPS 180
STANDARD. ~~SHALL BE AUTHENTICATED AND ENCRYPTED TO
A MINIMUM OF 128 BIT DES; [ADDITIONAL CRITERIA TO BE
DEVELOPED]~~

(D) ANY MODEM IN ANY COMPONENT FAILING TO MEET THIS
CRITERIA SHALL NOT BE USED BY ANY VOTING SYSTEM.

~~45.5.2.7.2 All electronic transmissions across public networks shall be
secured to the level and using the technologies prescribed in the
State of Colorado's "Minimum IT Architecture Standards" as
adopted by the Information Management Commission at the
time of certification. The voting system provider shall provide
documentation describing in detail the steps and methods used
for those electronic transmissions. This documentation will
describe, at a minimum, the methods by which authentication,
confidentiality, integrity, and availability of the transmission
and verification of electronically transmitted information will be
performed.~~

~~45.5.2.7.3 The voting system provider is required to provide to the SOS an
affidavit of compliance with the State's "Minimum IT
Architecture Standards" and is further required to indicate to the
State any variance(s) between the vendor's systems and the
State's standards within the documentation submitted for
certification of the voting system.~~

~~45.5.2.7.4 Any system that incorporates wireless transmission shall include
a detailed security plan specific to the wireless protocol being
deployed with the voting system. The detailed plan shall
include specific instructions for end users of the system to allow~~

1   ~~passwords and security keys to be set and/or generated by the~~
2   ~~end user.~~

3   45.5.2.7.3   ALL WIRELESS COMPONENTS ON VOTING SYSTEMS SHALL BE
4   DISABLED WITH THE EXCEPTION OF LINE OF SIGHT INFRARED
5   TECHNOLOGY USED IN A CLOSED ENVIRONMENT WHERE THE
6   TRANSMISSION AND RECEPTION IS SHIELDED FROM EXTERNAL
7   INFRARED SIGNALS AND CAN ONLY ACCEPT INFRARED SIGNALS
8   GENERATED FROM WITHIN THE SYSTEM.

9   45.5.2.7.~~5~~4   All systems that transmit data over public telecommunications
10   networks shall maintain a clear audit trail that can be provided
11   to the SOS when election results are transmitted by telephone,
12   microwave or any other type of electronic communication.

13   45.5.2.7.~~6~~5   Systems designed for transmission of voter information (i.e.
14   electronic pollbooks) over public networks shall meet security
15   standards that address the security risks attendant with the
16   casting of ballots at remote sites controlled by election officials
17   using the voting system configured and installed by election
18   officials and/or their voting system provider or contractor, and
19   using in-person authentication of individual voters.

20   45.5.2.7.~~7~~6   Any voting system provider of systems that cast individual
21   ballots over a public telecommunications network shall provide
22   detailed descriptions of:

23   (a)   All activities mandatory to ensuring effective system
24   security to be performed in setting up the system for
25   operation, including testing of security before an election.

26   (b)   All activities that should be prohibited during system setup
27   and during the time frame for voting operations, including
28   both the hours when polls are open and when polls are
29   closed.

30   45.5.2.7.7   IN ANY SITUATION IN WHICH THE VOTING SYSTEM PROVIDER'S
31   SYSTEM TRANSMITS DATA THROUGH ANY TELECOMMUNICATIONS
32   MEDIUM, THE SYSTEM SHALL BE ABLE TO RECOVER, EITHER
33   AUTOMATICALLY OR WITH MANUAL INTERVENTION, FROM
34   INCOMPLETE OR FAILED TRANSMISSION SESSIONS AND RESUME
35   TRANSMISSIONS AUTOMATICALLY WHEN TELECOMMUNICATIONS
36   ARE RE-ESTABLISHED.

37   (A)   RECOVERY OF TRANSMISSIONS SHALL INCLUDE NOTATIONS
38   OF THE INTERRUPTED TRANSMISSION SESSION AND THE
39   RESUMED TRANSMISSION SESSION IN THE SYSTEM AND
40   APPLICATION TRANSACTION LOGS.

Formatted: Small caps

Formatted: Indent: Left: 1.63", Hanging: 0.88", Tab stops: Not at 2.88"

(B) FAILURE AND RECOVERY OF TRANSMISSIONS SHALL NOT CAUSE ANY ERROR IN DATA TRANSMITTED FROM THE POLLING PLACE TO THE CENTRAL ELECTION SITE DURING A RECOVERED TRANSMISSION SESSION.

45.5.2.8 Accessibility Requirements

45.5.2.8.1 Specific minimum accessibility requirements include those specified in section §1-5-704 C.R.S., SOS Rule 34, Rule 35 and the following:

(a) Buttons and controls shall be distinguishable by both shape and color.

(b) Audio ballots shall meet the following standards:
1. The voting system shall allow the voter to pause and resume the audio presentation.
2. The audio system shall allow voters to control within reasonable limits, the rate of speech.

(c) No voting system or any of its accessible components shall require voter speech for its operation.

45.5.2.8.2 Documentation of the accessibility of the voting system shall include the following items at a minimum:

(a) If appropriate, voting booth design features that provide for privacy for the voter while voting (if a voting booth is not included with the system, then describe how voter privacy is accomplished).

(b) Adaptability of the proposed system for voters with disabilities as outlined in the Americans with Disabilities Act guidelines.

(c) Technology used by the voting system that prevents headset/headphone interference with hearing aids.

(d) Types and size of voice file(s) the voting system uses.

(e) Method for recording, sharing and storing voice files in the voting system.

(f) How paginating through viewable screens is accomplished if it is required with the voting system.

(g) Various methods of voting to ensure access by persons with multiple disabilities. Voting systems shall include

push buttons, keypad, "puff-sip" tube, touch screen, switches, and blink control devices.

(h) Capabilities of the voting system to accurately accept a non-human touch as input on the touch screen.

(i) User adjustability of color settings, screen contrasts, and screen angles/tilt if the system uses a display screen.

45.5.2.9 Voter-Verifiable Paper Record Requirements(V-VPAT)

45.5.2.9.1 V-VPAT shall refer to a Voter-verified paper record as defined in section1-1-104(50.6)(a), C.R.S.

45.5.2.9.2 Existing systems that are retrofitted to comply with this law shall be certified by the SOS. Any retrofitted voting system shall comply with the process and application for certification as identified by this rule.

45.5.2.9.3 The V-VPAT shall consist of the following minimum components:

(a) 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) 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.

(c) The V-VPAT unit shall contain a paper record storage unit that shall store cast and spoiled paper record copies securely.

(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 upon the completion of casting a ballot.

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.

45.5.2.9.6   The printer shall not be permitted to communicate with any other device than the voting device to which it is connected.

45.5.2.9.7   The printer shall only be able to function as a printer, and not perform any other services or possess network capability.

45.5.2.9.8   Every electronic voting record shall have a corresponding paper record.

45.5.2.9.9   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.

45.5.2.9.10   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.

45.5.2.9.11   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   The V-VPAT printer shall print at a font size no less than ten (10) points 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   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 they voted in on the DRE.

45.5.2.9.14   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   The V-VPAT system shall be capable of printing and storing paper record copies for at least 150 ballots cast without requiring the paper supply source, ink or toner supply, or any other similar consumable supply to be changed during the voting period, assuming a fully printed double sided eighteen (18) inch ballot.

45.5.2.9.16   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

1   allowed to reprint and review the paper audit trail without
2   having to re-mark his or her ballot, and the device shall prevent
3   the election judge from seeing any voters' ballots.

4 45.5.2.9.17 The voting system provider shall provide procedures and
5   documentation for the use of the V-VPAT device.

6 45.5.2.9.18 The printed information on the printed ballot or verification
7   portion of the V-VPAT device shall contain at least the
8   following items:

9   (a) Name or header information of race, question or issue

10   (b) Voter's selections for the race information.

11   (c) Write-in candidate's names if selected.

12   (d) Undervote or overvote information – this is in addition to
13   the information on the review screen of the DRE.

14   (e) Unique serial number (randomized to protect privacy)

15   (f) Identification that the ballot was cancelled or cast

16 45.5.2.9.19 The V-VPAT shall allow a voter to spoil his or her paper record
17   no more than two (2) times. Upon spoiling, the voter shall be
18   able to modify and verify selections on the DRE without having
19   to reselect all of his or her choices.

20 45.5.2.9.20 Before the voter causes a third and final record to be printed, the
21   voter shall be presented with a warning notice that the selections
22   made on screen shall be final and the voter shall see and verify a
23   printout of his or her vote, but shall not be given additional
24   opportunities to change their vote.

25 45.5.2.9.21 All V-VPAT components shall be capable of integrating into
26   existing state testing and auditing requirements of the voting
27   system.

28 45.5.2.9.22 The V-VPAT component should print a barcode with each
29   record that contains the human readable contents of the paper
30   record and digital signature information. The voting system
31   provider shall include documentation of the barcode type,
32   protocol, and/or description of barcode and the method of
33   reading the barcode as applicable to the voting system.

34 45.5.2.9.23 The V-VPAT component shall be designed such that a voter
35   may 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 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 section1-8.5-108(2), C.R.S.

45.5.2.9.25 The SOS shall keep on file procedures submitted by the voting system provider for how to investigate and resolve malfunctions including, but not limited to: 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.

45.6 Testing

45.6.1 Voting System Provider Demonstration

45.6.1.1 The voting system provider shall demonstrate the exact proposed voting system to the SOS or his or her designee prior to any functional testing. It should be expected that a minimum of 6 hours would be required of the voting system provider to demonstrate and assist with programming of the software as necessary.

45.6.1.2 The demonstration period does not have a pre-determined agenda for the voting system provider to follow, however, presentations should be prepared to address and demonstrate with the specific system the following items as they pertain to each area and use within the voting system:

(a) System overview

(b) Verification of complete system matching EAC certification

(c) Ballot definition creation

(d) Import EML file from statewide voter registration system

(e) Printing ballots on demand

(f) Hardware diagnostics testing

(g) Programming election media devices for various count methods:

● Absentee

● Early Voting

● Precinct/Poll Place

● Provisional

1   ●   Vote Center

2   (h)   Sealing and securing system devices

3   (i)   Logic and accuracy testing

4   (j)   Processing ballots

5   (k)   Accessible use

6   (l)   Accumulating results

7   (m)   Post-election audit

8   (n)   Canvass process handling

9   (o)   Audit steps and procedures throughout all processes.

10   (p)   Certification of results (export EML to statewide voter registration
11   system)

12   (q)   Troubleshooting.

13   45.6.1.3 The voting system provider shall have access to the demonstration room for
14   one hour prior to the start of the demonstration to provide time for setup of
15   the voting system.

16   45.6.1.4 A maximum of 3 business days – 24 hours total shall be allowed for the
17   demonstration.

18   45.6.1.5 The demonstration shall be open to representatives of the press and the public
19   to the extent allowable. The SOS may limit the number of representatives
20   from each group to accommodate space limitations and other considerations.

21   45.6.1.6 The SOS shall post notice of the fact that the demonstration will take place in
22   the designated public place for posting notices for at least seven (7) days
23   before the demonstration. The notice shall indicate the general time frame
24   during which the demonstration may take place and the manner in which
25   members of the public may obtain specific information about the time and
26   place of the test.

27   45.6.1.7 THE VOTING SYSTEM PROVIDER SHALL PROVIDE THE SAME CLASS OF
28   WORKSTATION AND/OR SERVER FOR TESTING THE VOTING SYSTEM AS THE
29   NORMAL PRODUCTION ENVIRONMENT FOR THE STATE OF COLORADO.

30   45.6.1.8 THE PROPRIETARY SOFTWARE SHALL BE INSTALLED ON THE WORKSTATION BY
31   THE TESTING BOARD FOLLOWING THE DOCUMENTATION PROVIDED BY THE
32   VOTING SYSTEM PROVIDER AFTER THE ESTABLISHMENT OF THE "TRUSTED
33   BUILD."

1   45.6.2 Functional Testing

2   45.6.2.1   Voting system provider requirements for testing

3   45.6.2.1.1   The voting system provider shall submit for testing the specific
4   system configuration that shall be offered to end users
5   JURISDICTIONS including the components WITH WHICH the voting
6   system provider recommends THAT to be used with the system
7   BE USED.

8   45.6.2.1.2   The voting system provider is not required to be present for the
9   functional testing, but shall provide a point of contact for
10   support.

11   45.6.2.1.3   The voting system provider shall DEPOSIT WITH THE SECRETARY
12   OF STATE THE "TRUSTED BUILD" provide a copy of the version
13   being certified of software, firmware, utilities, hardware and
14   instructions to install, operate and test the system being
15   submitted for certification.

16   45.6.2.1.4   The test shall be performed with test ballots and an election
17   setup file, as determined by the SOS.

18   45.6.2.1.5   Functional testing shall be completed within 17 days of the
19   successful conclusion of the voting system provider
20   demonstrationACCORDING TO THE SCHEDULE IDENTIFIED IN
21   SECTION 45.3.3.

22   45.6.2.2 SOS requirements for testing

23   45.6.2.2.1   The SOS or the designee shall conduct functional testing on the
24   voting system based on this rule and additional testing
25   procedures as determined by the SOS.

26   45.6.2.2.2   The voting system shall receive a pass/fail for each test
27   conducted WITH APPLICABLE NOTATION ON THE TEST LOG.
28   [ADDITIONAL REQUIREMENTS TO BE DEVELOPED]

29   45.6.2.2.3   A TEST log of the testing procedure shall be maintained and
30   recorded on file with the SOS. This TEST log shall identify the
31   system and all components by voting system provider name,
32   make, model, serial number, software version, firmware
33   version, date tested, test number, test description, notes of test,
34   APPLICABLE TEST SCRIPTS, and results of test. All test
35   environment conditions shall be noted.

45.6.2.2.4   All operating steps, the identity and quantity of simulated ballots, annotations of output reports, and observations of performance shall be recorded.

45.6.2.2.5   In the event that a deviation to requirements pertaining to the test environment, voting system arrangement and method of operation, the specified test procedure, or the provision of test instrumentation and facilities is required, this deviation shall be recorded in the test log together with a discussion of the reason for the deviation and a statement of the effect of the deviation on the validity of the test procedure.

45.6.2.3 General Testing Procedures and Instructions

45.6.2.3.1   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)   Verify, by means of applicant's standard operating procedure, that the device is in a normal condition and status.

(b)   Establish the standard test environment or the special environment required to perform the test.

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

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

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

45.6.2.3.2   All tests shall be conducted as described in this section 45.6.2.3 in regular election mode. At no point shall testing be conducted in any form of test mode.

45.6.2.3.3   Each voting system shall be tested and examined by conducting a TWO mock ELECTIONS – A PRIMARY, AND A coordinated election.

45.6.2.3.4   Each component of the voting system shall contain provisions for verifying it is functioning correctly and, whether operation of the component is dependent upon instructions specific to that election.

45.6.2.3.5   Both election scenarios shall feature at least 10 districts (or district types), comprised of at least 20 precincts that will result in a minimum of 5 unique ballot styles or combinations.

45.6.2.3.6   The voting system provider is required to produce a minimum of 500 ballots for each of the two elections. Enough ballots need to be created to conduct the testing of the voting system as defined in this rule. One complete set of ballots will be tested in each of the applicable counter types (or groups) indicated below:

    (a)   Poll Place or Vote Center - ballots are flat – no score marks

    (b)   Early Voting – ballots are flat – no score marks

    (c)   Absentee – ballots are scored and folded to fit in standard Colorado Absentee Mailing Envelopes.

    (d)   Provisional – ballots are flat- no score marks

45.6.2.3.7   The voting system provider shall pre-mark all ballots used for testing, with the exception of at least 175 blank ballots that shall represent 5 blank ballots for every precinct and precinct-split based on the programming mentioned in this section 45.6.2.3. Pre-marked ballots shall also have a predetermined tally that the voting system provider shall provide to the SOS for the testing of the ballots. Markings shall represent all of the testing scenarios as described in this rule.

45.6.2.3.8   The voting system provider shall provide 10 ballot marking pens/pencils/markers as defined by their system for marking ballots by the SOS or the designee.

45.6.2.3.9   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), Absentee, Provisional, and Early Voting. Ballots may be run through components 10 or more times 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   =   1,500

    (b)   Polling Place / DRE   =   500

    (c)   Vote Center/ OS   =   5,000

1	(d)	Vote Center / DRE	=	500
2	(e)	Early Voting / OS	=	5,000
3	(f)	Early Voting / DRE	=	250
4	(g)	Absentee	=	10,000
5	(h)	Provisional	=	5,000

45.6.2.3.10 Ballot design shall cover the scope of allowable designs for the given system. For example, if a system is capable of producing 11" and 18" ballots, then both ballot styles shall be tested in each of the elections above. If more sizes are available, they shall also be tested. BALLOTS MUST BE DESIGNED AND PRESENTED WITH A MAXIMUM OF FOUR (4) COLUMNS AND A MINIMUM OF ONE (1) COLUMN.

45.6.2.3.11 Ballots shall be printed in applicable languages as required by state and/or federal law.

45.6.2.3.12 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.

45.6.2.3.13 Ballots shall include the following minimum race situations to simulate and test "real world" situations in the State of Colorado:

(a) Parties for different races.

(b) Selection of a pair of candidates (i.e. president and vice president)

(c) In a Primary Election, allow a voter to vote for the candidate of the party of his or her choice and for any and all non-partisan candidates and measures, while preventing the voter from voting for a candidate of another party.

(d) 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 select any measure on the ballot that the candidate is allowed to vote in, regardless of party.

1   (e)   A minimum of 20 pairs of "yes" and "no" positions for
2   voting on ballot issues.

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

5   45.6.2.3.14 Additional tests and procedures may be requested at the
6   discretion of the SOS.

7   45.6.3 Failure Criteria

8   45.6.3.1 Voting systems shall successfully complete ~~all of~~ the requirements in this
9   rule, and any additional testing that is deemed necessary by the SOS.

10   45.6.3.2 If any malfunction or data error is detected, its occurrence and the duration of
11   operating time preceding it shall be recorded for inclusion in the analysis and
12   the test shall be interrupted. If corrective action is taken to restore the devices
13   to a fully operational condition within 8 hours, then the test may be resumed
14   at the point of suspension.

15 45.7   Temporary Use

16   45.7.1 If a voting system provider has a system that has been approved by an ITA, but has not
17   yet been approved for certification through the SOS, the voting system provider or the
18   designated election official may apply to the SOS for temporary approval of the
19   system to be used for up to one year.

20   45.7.2 Upon approval of temporary use, a jurisdiction may use the voting system, or enter
21   into a contract to rent or lease the voting system for a specific election upon receiving
22   written notice from the SOS's office. At no time shall a jurisdiction enter into a
23   contract to purchase a voting system that's been approved for temporary use.

24   45.7.3 The SOS shall approve use of a temporarily approved voting system for each election
25   that a jurisdiction would like to conduct with the voting system.

26   45.7.4 Temporary use does not supersede the certification requirements and/or process, and
27   may be revoked at any time at the discretion of the SOS.

28 45.8   Periodic Review

29   45.8.1 The SOS shall periodically review the voting systems in use in Colorado to determine
30   if the system(s):

31   (a) Are defective, obsolete, or unacceptable for use based on the requirements of this
32   rule.

33   (b) HAVE BEEN MODIFIED FROM C~~C~~ertified and ~~approved~~ "TRUSTED BUILD" versions of
34   hardware or software ~~have been modified~~.

1   ⸺ (e) The software matches with the software in escrow with the SOS.

2   45.8.2 The SOS shall review a minimum of two randomly selected jurisdictions and voting
3   systems per calendar year at the choosing of the SOS.

4   45.8.3 THE SOS SHALL CONDUCT AN ANNUAL VISUAL INSPECTION OF ALL SOFTWARE INCIDENT
5   RECORDS MAINTAINED BY EACH VENDOR CERTIFIED FOR USE IN THE STATE OF
6   COLORADO.

7   45.8.3̶4̶   After such review, certification or temporary approval for use may be
8   withdrawn. Three (3) months notice shall be given prior to withdrawing certification
9   of any voting system unless the SOS shows good cause for a shorter notice period.

10   45.8.4̶5̶   All forms, notes and documentation from a periodic review shall be kept on
11   file with the SOS.

12   45.9   Decertification

13   45.9.1 If after any time the SOS has certified a voting system, it is determined that the voting
14   system fails to meet the standards set forth in this rule, the SOS shall notify any e̶n̶d̶
15   u̶s̶e̶r̶s̶ JURISDICTIONS in the State of Colorado and the voting system provider of that
16   particular voting system that the certification of that system for future use and sale in
17   Colorado is to be withdrawn.

18   45.9.2 Certification of a voting system may be revoked and/or suspended at the discretion of
19   the SOS based on information that may be provided after the completion of the initial
20   certification. This information may come from any of the following sources:

21   (a) The Election Assistance Commission (EAC)

22   (b) Independent Testing Authorities (ITA)

23   (c) The Federal Election Commission (FEC)

24   (d) The National Software Reference Library (NSRL)

25   (e) National Association of State Election Directors (NASED)

26   (f) The National Association of Secretaries of State (NASS)

27   (g) Information from any state elections department or S̶O̶ ̶S̶SECRETARY OF STATE

28   (h) Information from Colorado County Clerk and Recorders or their association.

29   45.9.3 Any use of a decertified or uncertified voting system for any jurisdiction in the State of
30   Colorado shall result in possible loss of future and other existing certifications within
31   the state, at the discretion of the SOS.

32   45.9.4 Pursuant to section 1-5-621, C.R.S., the SOS shall hold a public hearing to consider

1   the decision to decertify a voting system.

2   45.10   Modifications and Re-examination

3   45.10.1   Any field modification, change, or other alteration to a voting system shall
4   require approval or certification before it may be used in any election within the State
5   of Colorado.

6   45.10.2   A voting system provider may apply to the SOS for the review of a
7   modification of an existing certified system at any time during the year. The voting
8   system is required to go through the complete certification process.

9   45.11   ACCEPTANCE TESTING BY JURISDICTIONS

10   45.11.1   WHENEVER AN ELECTION JURISDICTION ACQUIRES A NEW SYSTEM OR
11   MODIFICATION OF AN EXISTING SYSTEM CERTIFIED BY THE SOS, THE ELECTION
12   JURISDICTION SHALL PERFORM ACCEPTANCE TESTS OF THE SYSTEM BEFORE IT MAY BE
13   USED TO CAST OR COUNT VOTES AT ANY ELECTION. THE VOTING SYSTEM SHALL BE
14   OPERATING CORRECTLY, PASS ALL TESTS AS DIRECTED BY THE ACQUIRING
15   JURISDICTION'S PROJECT MANAGER OR CONTRACT NEGOTIATOR, AND SHALL BE
16   IDENTICAL TO THE VOTING SYSTEM CERTIFIED BY THE SOS.

17   45.11.2   THE VOTING SYSTEM PROVIDER SHALL PROVIDE ALL MANUALS AND TRAINING
18   NECESSARY FOR THE PROPER OPERATION OF THE SYSTEM TO THE JURISDICTION, OR AS
19   INDICATED BY THEIR CONTRACT.

20   45.11.3   THE ELECTION JURISDICTION SHALL PERFORM A SERIES OF FUNCTIONAL AND
21   PROGRAMMING TESTS THAT SHALL TEST ALL FUNCTIONS OF THE VOTING SYSTEM AT
22   THEIR DISCRETION.

23   45.11.4   THE JURISDICTION SHALL COORDINATE ACCEPTANCE TESTING WITH THE SOS'S
24   DESIGNATED AGENT AND COMPLETE A JURISDICTION ACCEPTANCE TEST form
25   PROVIDED BY THE SOS.

26   ~~45.11.5   ACCEPTANCE TESTING IS AT THE DISCRETION OF THE PURCHASING JURISDICTION,~~
27   ~~HOWEVER, IF THE JURISDICTION CHOOSES TO WAIVE THE OPPORTUNITY TO CONDUCT~~
28   ~~ACCEPTANCE TESTING OF THE VOTING SYSTEM THEY ARE PURCHASING, SUCH~~
29   ~~INDICATION SHALL BE MADE ON THE JURISDICTION ACCEPTANCE TEST FORM..~~

30   45.~~11~~12   Purchases and Contracts

31   45.~~11~~12.1   Any voting system that has been certified under the procedures of this Rule are
32   eligible for purchase, lease, or rent for use by jurisdictions within the State of
33   Colorado ~~upon written approval by the SOS of the contract between the jurisdiction~~
34   ~~and the voting system provider~~ PROVIDING THE CONTRACT CONTAINS THE FOLLOWING
35   ITEMS:~~:~~

36   ~~45. 1112.2   At the completion of contract negotiations, a jurisdiction entering into a~~

1   contract to purchase, lease or rent a voting system for use in the State of Colorado
2   shall request approval of the contract from the SOS prior to signing the contract.

3   45. 1112.3   The SOS or his or her designee shall approve the contract based on the
4   following minimum criteria:

5   (a) The voting system is certified for use within the State.

6   (b) Contract contains training and maintenance costs for Jurisdiction.

7   (c) Contract identifies components contained in the certified voting system, and
8   appears complete with all accessories necessary for successfully conducting an
9   election within the laws and rules of the State of Colorado.

10 (d) The voting system and associated components are purchased at or below the
11 following costs:

12

Item and Description	Maximum Contracted Cost
Ballot Tabulation Only Software	$48,000.00
Complete Software Package	$420,000.00
DRE with V VPAT	$7,000.00
DRE without V VPAT	$5,000.00
DRE Card Activator or Programmer	$3,000.00
DRE Disabled Devices attachment	$1,000.00
Extended DRE Warranty Per unit Per Year	$2,000.00
Precinct/Vote Center Level Optical Scanner	$7,000.00
High Speed Absentee Scanner	$120,000.00
Card Reader/Device to complete tabulation	$7,000.00
Extended Warranty Per scanner unit Per Year	$10,000.00
Yearly Maintenance	$108,000.00
Ballot Programming Charges (complete)	$65,000.00
Memory Cards or Cartridges (each)	$1,000.00

13 45. 1112.4   The SOS shall take no more than three (3) business days FORTY EIGHT (48)
14 HOURS to review the contract and return a decision to the corresponding jurisdiction.

15 45. 1112.5   The SOS shall annually review the costs in the table in section 45. 1112.3 and
16 update it as necessary.

17 45. 1112.6   The SOS shall maintain on file a list of all components used and purchased for
18 use. The list shall include at a minimum, the name of the jurisdiction, the date of
19 purchase, the serial number(s) of voting devices and voting systems that was
20 purchased.

21 45. 1112.7   Additionally, the voting system provider shall, through the process of this rule,
22 complete and negotiate with the SOS a purchase price agreement for counties to use when
23 purchasing equipment in the State of Colorado. The pricing agreement shall:

1   (a)   Be valid for one year from the date of certification;

2   (b)   Require renegotiations at the end of the pricing agreement period to continue future
3   sales within the state;

4   (c)   Allow counties to purchase equipment listed on the agreement at the agreed upon
5   price for the duration or to negotiate directly with the voting system provider for a potentially
6   lower price; and

7   (d)   Be inclusive of the best costs the voting system provider is willing to sell all
8   components, including any support, warranty or maintenance costs of the system being
9   certified through this rule.