STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Mike Coffman
Secretary of State

Holly Z. Lowder
Director, Elections Division

NOTICE OF ADOPTION

Pursuant to sections 1-1-107(2)(a) and 1-1.5-104(1)(e), C.R.S. (2006) and the rulemaking provisions of the State Administrative Procedure Act, section 24-4-103 C.R.S. (2006), I, Mike Coffman, Colorado Secretary of State, do hereby adopt and give **NOTICE** of the temporary and permanent rule adoption this 16th day of March, 2007, of the amendments to the attached Secretary of State Election Rules (8 CCR 1505-1).

Such amendments are effective immediately, and the permanent adoption of these rules shall take effect twenty (20) days after publication in the Colorado Register in accordance with the State Administrative Procedures Act. In accordance with section 24-4-103(6), C.R.S (2006), attached is a statement of the findings of the Secretary of State justifying the adoption of these amendments on a temporary basis.

Dated this 16th Day of March, 2007.

Mike Coffman
Colorado Secretary of State

Main Number (303) 894-2200
Administration (303) 860-6900
Fax - Administration (303) 869-4860
TDD (303) 869-4867
Web Site www.sos.state.co.us
E-mail – Administration sos.admin1@sos.state.co.us

STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Mike Coffman
Secretary of State

Holly Z. Lowder
Director, Elections Division

Statement of Justification and Reasons for Adoption of Temporary Rules

Office of the Secretary of State
Amended and Revised Rules 25.3, 26.2, 30.3, 38.10, 38.12, and 45
Colorado Secretary of State Election Rules
As Amended March 16, 2007

Under section 1-1-107(2)(b), C.R.S. (2006), the Secretary of State has the power "[t]o promulgate, publish, and distribute . . . such rules as the secretary of state finds necessary for the proper administration and enforcement of the election laws." In addition, section 1-1.5-104(1)(e), C.R.S. (2006), authorizes the Secretary of State to "[p]romulgate rules . . . as the secretary finds necessary for the proper administration, implementation, and enforcement of [the "Help America Vote Act of 2002", P.L. No. 107-252]."

On September 22, 2006, the Denver District Court ruled as follows: (1) "The Secretary is ordered to promulgate a rule containing minimum security standards for DREs as required by § 1-5-616(1)(g), C.R.S. (2006)." (2) "The Secretary is ordered to retest previously certified systems or any new systems, using the revised security standards to be promulgated by the Secretary, prior to the next primary, general or statewide ballot issue election following the November 7, 2006 general election, whichever comes first."

Certain amendments to the existing election rules are immediately necessary for the uniform and proper administration and enforcement of the election laws of the State of Colorado during the 2007 election cycle. These rules are specifically necessary in order to comply with the trial courts order in *Conroy v. Dennis*, No. 06CV6072 (Denver Dist. Ct.). Pursuant to that court order, the Secretary of State is required to promulgate voting systems certification rules that include minimum security standards for direct recording electronic voting systems and to retest all voting systems under such standard prior to the "next primary, general or statewide ballot issue election following the November 7, 2006 general election."

A statewide ballot issue election will be held in November 2007 if a qualified issue is placed on the ballot. The temporary adoption of the amendments and revisions to Election Rule 45 are necessary because all voting systems in use in Colorado must be tested under the revised security standards no later than July 1, 2007 in order to allow all county clerks in Colorado sufficient time to obtain approval for existing equipment, purchase any new equipment, and perform acceptance testing before the equipment is used in the election.

The Secretary of State finds that in order to ensure the uniform and proper administration and enforcement of the election laws, the adoption of the temporary amendments to the Secretary of State Election Rules is necessary both to comply with law and to preserve the public welfare generally.

Therefore, in accordance with section 24-4-103(6), C.R.S. (2006), the Secretary of State finds that temporary adoption of the amendments and revisions to existing election rules is "imperatively necessary to comply with a state or federal law or federal regulation or for the preservation of public health, safety, or welfare and compliance with the requirements of this section would be contrary to the public interest."

Main Number (303) 894-2200 Web Site www.sos.state.co.us
TDD (303) 869-4867 E-mail elections@sos.state.co.us
Fax (303) 869-4861

STATE OF COLORADO
Department of State
1700 Broadway
Suite 250
Denver, CO 80290

Mike Coffman
Secretary of State

Holly Z. Lowder
Director, Elections Division

Statements of Basis, Purpose and Specific Statutory Authority

Office of the Secretary of State
Amended and Revised Rules: 25.3, 26.2, 30.3, 38.10, 38.12, and 45
Election Rules

1. Basis and Purpose

This statement pertains to the amendments and revisions to the Colorado Secretary of State Election Rules for the administration of Colorado State Constitution Article VII, and Article 1, Title 1 of the Colorado Revised Statutes. The amendments are implemented to achieve the uniform and proper administration and enforcement of the election laws of the State of Colorado, specifically with regard to the requirements of the "Help America Vote Act of 2002", P.L. No. 107-252. See sections 1-1.5-101 *et seq.*, C.R.S. (2006).

The amendments and revisions to these rules are necessary for the implementation of Article VII of the Colorado Constitution and Article 1, Title 1 of the Colorado Revised Statutes. The Secretary of State finds that the adoption and enactment of these amendments and revisions is necessary in order to comply with a court order to promulgate voting systems certification rules that include minimum security standards for direct recording electronic voting systems.

Election Rule 45 is being revised pursuant to a court order *Conroy v. Dennis*, No. 06CV6072 (Denver Dist. Ct.) issued on September 22, 2006, which mandates that the Secretary must "promulgate a rule containing minimum security standards for DREs as required by § 1-5-616(1)(g), C.R.S. (2006)." The order further requires the Secretary "to retest previously certified systems or any new systems, using the revised security standards to be promulgated by the Secretary, prior to the next primary, general or statewide ballot issue election following the November 7, 2006 general election, whichever comes first." The Secretary of State finds that the adoption and enactment of the amendments and revisions to Rule 45 is necessary because a statewide ballot issue election may be held in November 2007 if a qualified issue is placed on the ballot.

The amendments and revisions to the Election Rule 45 must be adopted and implemented early in 2007 given the limited timeframe within which to test and certify voting equipment once the rules are effective. The state is required under section 1-5-617(1)(c), C.R.S., to conduct testing and certification within ninety days from the vendor's submission, and has an additional thirty days within which to make a report and notify the vendor and the counties of the determination. This process should be completed no later than July 1, 2007 in order to allow the county clerk and recorders sufficient time to obtain approval for and purchase any new equipment, and perform acceptance testing before the equipment is used in an election.

In drafting the revised Rule 45, the Secretary solicited the assistance of experts to identify specific security risks and define testing/certification requirements. The group included state and private sector IS/IT professionals, computer scientists, and university professors. Multiple drafting meetings were held involving the group IT/IS experts. The Secretary held an informal public meeting, in addition to the formal rulemaking hearing for the purpose of receiving public input on the draft rule. Following the formal rulemaking hearing held on February 6, 2007, the hearing record was held open for twenty days to allow for the submission of additional public comment. The comments received during and following the public meeting were considered in drafting the final Rule 45.

The Secretary of State finds that the adoption of the amendments and revisions to the Election Rules is further necessary to make technical corrections that have been requested by the Office of Legislative Legal Services, and to increase the transparency and security of the election process. The Secretary of State therefore finds that in order to ensure the uniform and proper administration and enforcement of the election laws, the permanent adoption of the amendments and revisions to the Election Rules is necessary both to comply with law and to preserve the public welfare generally.

This rule contains scientific and technical matters. The evaluation justifying scientific and technical rationale is as follows:

Background and Overview

Voting Equipment

Colorado currently has a variety of optical scan and Direct Recording Electronic (DRE) voting devices from one of four national vendors distributed as summarized in Figure 1 below.

	Counties	Voting Locations	% of voting locations	DREs	Optical Scanners	% of equipment
HART Intercivic	47	569	38%	1365	345	19%
DIEBOLD Election Systems	11	351	23%	1782	478	25%
SEQUOIA Voting Systems	4	356	24%	2355	270	29%
Election Systems and Software (ES&S)	2	231	15%	2267	124	27%
Grand Totals:	64	1,507		7769	1217	

Figure 1. 2007 Data on Voting Systems used in Colorado. http://www.elections.colorado.gov/DDefault.aspx?tid=113

Modern DRE devices fall into two categories; full face and ATM/Kiosk style units. The functionality of the units is the same; the presentation in the design of the unit is different. The full-face styled units allow all contests on a ballot to be displayed at once while the ATM/Kiosk style units require users to page through the contests in order to vote. The newer generation DREs (ATM/Kiosk) are distinguished by software platforms that are compatible with Windows operating systems and that interface with the voter to cast a ballot. Both styles feature redundant and removable memory on a standard memory card or cartridge, have the ability to present the ballot in different languages, and require some form of activation by a poll worker to "enable" the device for voting. The devices include voter activation cards which can be handled by the voter, activation codes which the voter can enter on a machine and activation devices which are

used by poll workers. All of the devices are designed to allow poll workers to provide the voter with the correct ballot style and to limit each voter to casting only one ballot.

Voting equipment used in Colorado must pass through several layers of security and testing. These requirements increase the quality, transparency and accuracy of votes as well as the public confidence and trust in the approval process for the devices and the accuracy of elections.

Federal Certification Process

Colorado Revised Statutes (C.R.S.) Section 1-5-601.5 requires the State to adopt and implement federal requirements for voting systems that are purchased for use within Colorado. The federal voting systems standards currently in effect are the 2002 Voting Systems Standards developed by the Federal Election Commission (FEC). All voting systems purchased for use in Colorado after May 28, 2004 must be tested and recommended for certification by a nationally approved Voting System Testing Laboratory (VSTL – formerly Independent Testing Authorities or "ITAs").

During federal certification, the VSTL will create a "trusted build" of the voting system which establishes the chain of evidence from the technical data package and source code to the actual computer programs and firmware that are being evaluated for certification. This chain of evidence will be sufficient to provide assurance that:

- The system was built as described in the technical data package;
- The reviewed and approved source code was actually used in building the system; and
- Elements that are not included in the technical data package are not introduced in the system build.

According to the Election Assistance Commission (EAC), the final product will provide the following:

> "The final product, the Trusted Build, provides an audited reference package, meeting legal rules of evidence in the form of a documented chain of custody, which may be used by technical reviewers at both the national and state level for certification." *Voting Systems Technical Guidelines Development Committee* (2006). Voting Systems Trusted Build – Guidelines.

State Certification Process

The Secretary of State's office has established new procedures and guidelines for Colorado's Trusted Build for the voting systems used in Colorado. In addition, the Secretary of State will conduct a review of the VSTL reports for compliance with federal and state regulations. The Secretary of State will create a trusted build for systems certified for use in Colorado where the VSTL or EAC has not already created a trusted build. Depending upon circumstances in each county, the Secretary of State will install, witness or document the trusted build software and firmware on all devices once the chain of evidence for the supporting documentation is established. (Secretary of State Rule 45.6.2.1.3, 8 CCR 1505-1) The Secretary of State intends that any system certified for use in Colorado will have extensive security put around the Colorado Trusted Build, and that the chain of evidence will be passed to the counties as indicated below.

County Acceptance Testing

The Secretary of State will be using the Colorado trusted build and shall install, witness and document the verification of the build for all equipment used in the State. The Secretary of State will provide the counties with tools to verify hash values (digital fingerprint of software) such as Tripwire® or Maresware® to perform software audit checking routinely to ensure and update the appropriate chain of evidence for county voting equipment. Upon validation of software and firmware, the county will perform acceptance testing with certification election data to ensure that field units match results found by the testing board for equipment used for certification testing. This procedure provides an additional level of trust in the equipment prior to the county moving into election processing.

County Security Requirements

The Secretary of State will continue to evaluate field security conditions and procedures necessary to maintain chain of custody (protect the integrity of voting equipment software, firmware and hardware). As systems are certified, specific new security procedures may be adapted and modified for systems based on the findings of the testing board. Secretary of State Rule 43, 8 CCR 1505-1 establishes minimum security procedures for all equipment in use throughout the State.

Election Testing and Audits

The Secretary of State provides guidance to the counties on conducting vigorous public pre-election testing (hardware diagnostics and logic and accuracy) which is intended to assure the public that the chain of custody over the software, firmware and hardware has been maintained. Pre-Election testing will utilize tools to verify the trusted build is being used on the device, and to validate that the election programming data is set up properly to count all votes as intended. In addition, the Secretary of State will conduct a mandatory post-election audit, randomly selecting 5% of all equipment used in the State. During the post-election audit, election administrators must verify that the paper record matches the count on the electronic record so that the Secretary of State can accept the electronic record as part of the certified results from any county.

Voter-Verifiable Paper Audit Trail (V-VPAT)

The V-VPAT creates the paper record that the voter verifies prior to casting a ballot. The V-VPAT record provides a layer of redundancy of vote records on all DRE machines which is in addition to the removable memory card, the physical hard drive of the device, and in some cases, a flash memory card located inside the machine. The record is not a receipt and cannot be removed from the voting location. The Colorado legislature mandated the V-VPAT for additional auditing capabilities needed with electronic voting systems to provide a method to assure voters that their votes are being accurately recorded by DRE devices (C.R.S. 1-5-801). The document created by the V-VPAT is considered an official election record used to qualify the electronic ballots in the case of a recount, and in the audit function required by the Secretary of State (C.R.S. 1-5-514). In addition to these functions, the V-VPAT record could be used to certify results of an election in any instance where the DREs security measures may have been compromised in any of the above steps.

Field Observations

As a final measure, the Secretary of State monitors equipment used. The Secretary of State uses field reports to evaluate whether any corrective action is necessary. After each election, the Secretary of State compiles malfunction reports received from the field and requires voting system vendors to provide detailed analysis with explanation and steps to prevent of malfunctions in the future. The Secretary of State's office reviews and audits county maintenance records throughout the year. In addition to these reports, the Secretary of State considers information from any of the following sources when considering certification status: The Election Assistance Commission (EAC); Voting Systems Testing Laboratories (VSTL); The Federal Election Commission (FEC); The National Software Reference Library (NSRL); The National Association of State Election Directors (NASED); The National Association of Secretaries of State (NASS); Information from any state elections department or secretary of state; and/or information from the Colorado County Clerk and Recorders or their association.

The Secretary of State employs a multi-layer process for handling the testing and security of voting systems used in the State. Several layers of testing and security procedures mitigate many of the risks associated with voting devices. Additionally, the Secretary of State includes the public to the extent possible during key moments in voting system testing and auditing by the counties.

Evaluated Threats and Vulnerabilities

The Secretary of State reviewed the following nationally known evaluations and reports on voting systems that have appeared over time. The following reports were evaluated. The Secretary of state has mitigated the vulnerabilities in Colorado as follows:

A. Brennan Center Report on Voting System Security, Accessibility, Usability, and Cost

On October 10, 2006, the Brennan Center for Justice released a report outlining a series of issues regarding voting systems security, accessibility, usability, and cost. With regard to security, the report identifies in the first chapter that all voting systems have significant security and reliability vulnerabilities which they indicate "can be substantially remedied if proper countermeasures are implemented at the state and local level." (Norden, 2006). The six recommended remedies include:

1. Conduct post-election audits comparing V-VPAT records to electronic records.
2. Perform parallel testing on election day.
3. Ban the use of wireless components on voting machines.
4. Use a transparent and random selection process for all auditing procedures.
5. Decentralize the programming and voting systems administration.
6. Implement procedures for addressing evidence of fraud or error.

The report determined the risks by creating a threat analysis which evaluated nine categories of threats and analyzed them against currently used systems by type, including evaluating DREs, optical scanners used in polling places, and central count optical scanners. The report finds that the least difficult attacks are software attacks involving the insertion of corrupt software in order to take over the voting machine and switch votes to a preferred candidate. Use of wireless

components makes systems particularly vulnerable to software attack programs and other attacks.

- The Secretary of State has implemented all but one of the recommendations of the Brennan Center report as follows:
    1. Post-Election Audits have been conducted since November of 2005 as required by statute and detailed out in Secretary of State Rule 11, 8 CCR 1505-1, which identifies that the V-VPAT record must be compared to the electronic record.
    2. For the mandatory post-election audit, the Secretary of State randomly selects machines to be audited without advance notice to the counties. The Secretary of State is evaluating methods to make this process more publicly transparent.
    3. Use of wireless components is banned in voting machines as identified in Secretary of State Rule 45, 8 CCR 1505-1.
    4. Programming and voting systems administration is decentralized because each county clerk is independently responsible for each of these functions. The Secretary of State is not involved with any functions related to the programming of voting equipment to ensure this decentralization. In addition there is an even distribution of the different manufacturers' voting products. Table 1.
    5. Through Secretary of State Rule 43, 8 CCR 1505-1, the State has implemented a series of procedures and remedies for handling voting equipment that may have evidence of fraud. The trusted build that is required under Secretary of State Rule 45.4, 8 CCR 1501-1, strengthens the effectiveness of these and future remedies because the Secretary of State will verify the current trusted state of the software and firmware of a machine, and may repeat this process once more on any machine that is suspected to be tampered with to ensure future use is safe and reliable. DRE equipment in the State also contains V-VPAT records which is used as the official record of votes for the election should machine tampering occur.
    6. The only recommendation not presently in place is parallel testing on election day. The Secretary is still evaluating the benefits of parallel testing and will amend procedures if deemed necessary in the future.

B. Analysis of an Electronic Voting System – "Hopkins Report"

On February 27, 2004, Johns Hopkins University released a report outlining security issues with the Diebold TS (also known as R6) DRE touch screen voting system. The main findings of the report indicate that through software exploits, voters can cast multiple ballots, easily gain access to administrative functions, and the system is overall lacking in security. Aside from a continuation of source code review, the only recommendation in the report was to mandate the addition of V-VPAT records with DRE voting devices.

- The analyzed system is no longer certified for use in the State of Colorado and V-VPAT records are required by statute. Thus, threats identified in the above report for that system are fully mitigated. However, the Secretary of State considered the concerns outlined in the report respective to other currently certified systems. The concerns are mitigated by V-VPAT requirements, random post-election audits aimed at identifying any discrepancies between paper and electronic records, implementing the trusted build mandate, requiring multiple tamper-evident seals on the case, doors and memory card slots of all DRE units to prevent unauthorized access.

C. Diebold Optical Scan Security Alert – Hursti Report 1

On July 4, 2005, Black Box Voting released a report outlining security issues with the Diebold Optical Scan (OS) design. The report identifies a one-man type of attack using commercial off-the-shelf technology. The attack requires unfettered inside access to the OS unit. Through this report, the author is capable of modifying the paper trail to report false results, hide any pre-loaded votes on the device, and program conditional reporting behavior based on time/date or number of votes counted triggers. Such attacks are done by modifying the reporting files on the OS unit or central tabulation software. The modifications would then be passed to other OS units either remotely or by direct connection to each one with the proper programming. Evidence of the tampering is not documented in the audit reports of the OS unit.

The recommended remedies are:

1. Further evaluation of the software architecture in Diebold version 1.96.x and 2.0.x.
2. Memory cards should be deemed to contain critical data and should be retained for 22 months following a federal election.
3. Memory cards and/or voting systems themselves should be examined in all jurisdictions using any Diebold voting system by someone experienced in computer forensics.
4. The architecture of other manufacturers should be examined for similar vulnerabilities.

- The Secretary of State has several layers of protection against the types of security issues identified in this report. The specific attack described affects the unofficial results report that is printed from the OS unit itself at the close of polls. However, even when this threat is realized, the accurate election results appear when an election administrator uploads the memory cards into the central count tabulator. The attack affects only the reporting function of the OS unit. Nonetheless, canvass reports will clearly show evidence of such an attack and would trigger a hand count of the paper records.

In addition to the above, the Secretary of State has other additional procedures in place to address this type of attack:

1. Colorado Bureau of Investigations background screens are required for individuals with this type of access to voting systems and memory cards. If the background screen indicated that the employee or contract employee has been found guilty of a crime involving breach of trust, fraudulent, coercive, or dishonest practices or demonstrating incompetence, untrustworthiness, or election offenses pursuant to sections 1-13-101 *et seq.*, C.R.S., the county clerk and recorder shall prohibit such employee or contract employee from preparing, programming, operating, using or having any access whatsoever to electromechanical voting systems or electronic vote tabulating equipment at any time during that person's employment. These screens are performed annually, and anyone with such access must be deputized to uphold the constitutions of the United States and Colorado in the execution of their duties.
2. Memory cards are sealed upon downloading data, and are secured by tamper-evident seal when in a voting device. The required seals must be checked and verified by at least two people as in place. Seals must be numbered and verified on chain of custody documentation maintained by the county.

3. Random post-election audits are conducted verifying the V-VPAT paper ballot to the report printed by the device on election night.
4. The Colorado trusted build will reset each component of a voting system to the trusted state after Secretary of State Certification of each device, and upon upgrades to the system.

D. Diebold TSx Evaluation – Hursti Report 2

On May 11, 2006, Black Box Voting released a report outlining security issues with the Diebold TSx touch screen voting machine. The study describes a method of enabling a malicious person to compromise the equipment well in advance of actually using the exploit. The report identifies three specific security problems associated with this threat. First, the system architecture makes it possible for an individual to modify files by changing the boot loader operation. This is known as boot loader re-flashing (or rebooting). In addition, the operating system may be modified through a process of re-flashing. Finally, the system architecture makes it possible to use either of the two previous methods to perform selective file replacement to modify the voting system software undetected.

Other weaknesses involve the internal workings of the system. By removing the six screws that hold the case together, an individual may access additional memory card slots including a "hidden" or at least unlabeled Secure Disk (SD) memory card slot. Files and/or programs could be installed modifying certified code on the system by gaining access to these ports.

The recommended remedies are to:
1. Re-flash all systems with a known good version;
2. Establish extensive chain of custody management;
3. Re-engineer the boot loader program; and
4. Properly seal the case.

- The Secretary of State implemented various methods of addressing these issues, including: sealing the four sides of a case to prevent opening with tamper-evident seals, extensive chain of custody procedures, and installation of a trusted build version to ensure no changes are made to the software and firmware components of the voting system. The Secretary of State has anticipated software issues such as the boot loader program and has added requirements in the Colorado certification process.

E. Princeton Report on the Security of the Diebold AccuVote TS Voting Machine

On September 13, 2006, Princeton University released a report outlining security vulnerabilities in the Diebold AccuVote Touch Screen (TS) voting machine. The focus of the study involves the TS Voting unit (also known as the R6) from Diebold which is not used in the State of Colorado. The report identifies two classes of attack, the Vote Stealing attack, and the Denial of Service attack. Both classes of attack could be conducted by introducing malicious code through the memory card via electronic election data card, or by introducing virus type spreading software onto the EPROM chip located on the motherboard (which effectively could spread to any memory card inserted into the unit).

Additional weaknesses in security involve key access to the memory card slot, modification of the boot loader files, and upgrades made to the machine via memory card. These vulnerabilities could go undetected with proper programming.

The reports main findings are as follows:

1. Malicious software running on a single voting machine can steal votes with little, if any, risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. The author of the Princeton Report has constructed demonstration software that carries out this vote-stealing attack.

2. Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. In practice, poll workers and others often have unsupervised access to the machines.

3. AccuVote-TS machines are susceptible to voting-machine viruses—computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre and post-election activity. The author of the Princeton Report has constructed a demonstration virus that spreads in this way, installing their demonstration vote-stealing program on every machine it infects.

4. While some of these problems can be eliminated by improving Diebold's software, others cannot be remedied without replacing the machines' hardware. Changes to election procedures would also be required to ensure security.

The report concludes the best methods to overcome these vulnerabilities are recommended as follows:

1. Modification of software and hardware to current federal standards;
2. Use tamper-evident seals on memory card access doors and slots;
3. Parallel testing DREs on election day;
4. Implement stronger certification procedures to evaluate source code;
5. Identified as the most important mitigation: Require V-VPAT and post-election random audits.

- The Diebold TS (R6) touch screen DRE is no longer certified for use in the State of Colorado. However, it is important for voter confidence to identify the solutions, the Secretary of State has already implemented in Colorado due to the high visibility of these reports. Colorado currently requires tamper-evident seals on memory cards and access door slots and an advanced chain of custody that the counties must maintain for the life of the equipment. Through this rule the Secretary of State is implementing more stringent standards for certification that include an additional source code review and penetration tests. As the report indicated, the most crucial mitigation is V-VPAT and post-election random audits, both of which are required in Colorado. The Secretary of State is still evaluating the benefits of parallel testing on election day. In addition, through Rule 45, 8 CCR 1505-1, the Secretary of State is requiring installation of a trusted build version followed by strict chain of custody requirements to ensure no changes are made to the software and firmware components of the voting system.

F. UConn Security Assessment of the Diebold OS Voting Terminal.

On October 30, 2006, the UConn VoTeR Center and Department of Computer Science and Engineering Department of the University of Connecticut released a report outlining security vulnerabilities in the Diebold AccuVote Optical Scan (OS) unit. This unit and the associated 1.96.6 firmware are certified for use in the State of Colorado. The report outlines and identifies a basic attack with several different outcomes including, neutralizing one candidate so that their votes are not counted, swapping the votes of two candidates, or biasing the results by shifting some votes from one candidate to another. The tabulation corruptions can lay dormant within the system, avoiding detection through pre-election tests. The report shows that these attacks can be conducted using only commercial off-the-shelf equipment and without any access to the memory card or physically opening the OS unit.

The report prescribes the following "safe-use" recommendations for the OS Unit:

1. Tamper-evident seals protecting removable memory card ports when in use and not in use;
2. Tamper-evident seals protecting all communications ports on back of unit; and
3. Tamper-evident seals over screws that allow access into the terminal's interior.

Alternatively, a jurisdiction could seal the entire OS unit into a tamper-resistant container at all times when not in use for preparation of election and deployment in election. An unbroken chain of custody must be enforced at all times, and post-election audits are advised.

- The Secretary of State has implemented the report's recommendations to conduct post-election audits, maintain unbroken chain of custody, and tamper-evident seals over the seams of the OS Unit. Additionally the Secretary of State will implement new county security procedures (Secretary of State Rule 43, 8 CCR 1505-1) which will require either sealing the entire unit in a case, or additional tamper-evident seals as recommended by the report.

Expert Panel Findings

The Secretary of State assembled a panel of provide advice concerning the security of electronic voting devices in Rule 45, 8 CCR 1505-1. The experts include nationally known experts on voting systems who have assisted in the development of federal testing procedures, have performed security audits on voting systems and assisted states such as Maryland, Pennsylvania, California, and Florida to draft standards for certification and in some cases conduct certification tests. Additionally, the panel consisted of computer scientists from Denver University Computer Science Department, University of Colorado Computer Science Department, and security experts from the Colorado Office of Cyber Security.

The security recommendations of the expert panel are as follows:

A. Federal Testing and Requirements

1. The expert panel recommended that the Secretary of State's office continue to adopt federal guidelines where appropriate while at the same time avoid duplicating the efforts of the EAC/VSTL process. Because some of the federal requirements are not specific to Colorado needs, and because some portions of the federal standards will not be implemented until a future date, the State must

implement its own procedures for source code review and software coding standards in a manner that allows the state to comply with federal and state standards.

- The Secretary of State has adopted many procedures for source code review, coding standards, security and hardening of operating systems, databases and communications devices as identified below with significant discussion by the expert panel.

B. Implementation of Multiple Layers of Security

1. The expert panel recommended that the Secretary of State's office adopt procedures and requirements that build upon each other in a layering fashion. In particular, the first layer of security is the trusted build, including the verification of the build itself as well as the chain of evidence documents related thereto. Additionally, experts recommended that the Secretary of State or his designee install, witness or document the installation of the trusted build onto the equipment. After completing installation, witnessing the installation, or documenting the installation, the experts recommended that the Secretary of State or his designee immediately validate the versions and build numbers installed against trusted configurations. This is intended to ensure that all prior builds on the voting equipment are eliminated and that only the Secretary of State's authorized and trusted build is utilized on voting systems used in the State of Colorado.

   - The Secretary of State implemented this recommendation in Rule 45, 8 CCR 1505-1 (section 45.6.2.1.3). The Secretary of State will witness, install or document the verification of all voting devices in the State to be of the same version as the trusted build through either reformat of device, rebuild of device, or hash valued verification/CRC check of the components. This procedure will be documented and to the extent possible video recorded.

2. The expert panel also recommended an independent source code review against known coding standards for hardened systems. The experts recommended a review of the vendors' source code to standards provided from the National Institute for Standards and Technology (NIST), National Security Agency (NSA) and/or manufacturers of certain software. As these standards are continually updated, the experts recommended the analysis be to presently known coding standards. As recommended by the expert panel, the source code review should include specific known NIST developed guidelines for software hardening which include: input validations, range errors, API abuses, Time and State conditions, code quality conditions, and encapsulation conditions.

   - The Secretary of State implemented this recommendation in Rule 45, 8 CCR 1505-1 (section 45.5.2.4.3).

3. The expert panel also recommended an independent penetration test be conducted on the software to the Open Source Security Testing Methodology Manual

(OSSTMM) 2.2 standards as defined for white box or double gray box testing, which provides:

> "In white box testing, the auditor engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is notified in advance of the scope and timeframe of the audit but not the channels tested or the test vectors. A double gray box audit tests the skills of the auditor and the target's preparedness to unknown variables of agitation. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the auditor and the target before the test as well as the auditor's applicable knowledge." Herzog, Peter (2006). *OSSTMM 2.2. - Open-Source Security Testing Methodology Manual.* P12.

- The Secretary of State implemented this recommendation in Rule 45, 8 CCR 1505-1 (section 45.5.2.4.3).

4. The expert panel recommended the Secretary of State consider and mitigate known risk and threat models by implementing additional conditions on certifications, increased county security measures or other restrictions as necessary on a case by case basis. The experts generally recommended that the Secretary of State allow himself reasonable discretion to do this, as well as to address other minor concerns with the voting systems. The experts explained this recommendation is based upon the reality that the systems are unique and each may raise distinct issues that can be reasonably addressed through procedures.

   - The Secretary of State implemented this recommendation in Rule 45, 8 CCR 1505-1 (section 45.5.2.4.3).

5. The expert panel recommended increased county acceptance testing and State oversight of the distribution of the trusted build. As stated earlier, the experts recommended the Secretary of State install, observe or document the installation and validation of the trusted build on the county equipment. The expert panel recommended that, immediately after this step the Secretary of State mandate and enforces acceptance testing of the systems at the moment of the installation of the trusted build and documents the results of acceptance testing.

   - The Secretary of State implemented this recommendation in Rule 45, 8 CCR 1505-1 (section 45.11). At the time of distribution and documentation of the trusted build, the Secretary of State will conduct acceptance testing of the device using ballots and election files from certification testing with known outcomes to verify proper operation of the device.

C. Specific Security Requirements

The Secretary of State requested the expert panel to make recommendations for security requirements that should be adopted as part of the process for certification of voting systems. The following sections represent the findings of the expert panel:

1. Access Controls. The expert panel suggested restricting access to the voting system to the least amount of privilege possible for the system. The layers of account access include: Operating System Administrative Account, Operating System User Account, Voting System Application Administrative Account, and Voting System Application User Account. Specifically, the panel recommended restricting the Operating System Administrative Account from having the ability to delete or modify the election database. With tightly restricted access controls, this known risk is mitigated.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(a).

2. Network Security. The expert panel recognized the need for elections administrators to use the election management software in a closed, non-routable, non-traceable environment where peripheral devices may be attached at various times in the process. The experts recommended the Secretary of State clearly define a closed network and ensure that the networks are restricted to allow only the above network activity items.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(b) and used the definition provided by the expert panel for closed network.

3. Database Security. The expert panel recommended implementing database hardening to accepted industry standards that have been developed by either the NSA or NIST.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(c) using guidelines currently adopted by the NSA.

4. Operating System Security. The expert panel recommended implementing operating system hardening to accepted industry standards that have been developed by either the NSA or NIST.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(d) using guidelines currently adopted by the NSA.

5. Password Security. The expert panel evaluated the use of passwords in various components of the voting system and recommended strengthening for password requirements to a minimum of eight characters, including a combination of alpha and numeric and possibly special characters. Additionally, the panel recommended restricting the use of administrator level passwords on all components for normal activity, requiring the use of separate passwords for user level functions, and prohibiting the use of blank passwords.

   - The Secretary of State implemented all of these recommendations in section 45.5.2.6.1(e). Based on feedback provided by the experts, the Secretary of State determined that in order to adequately implement the eight character password, that design changes to the voting systems may be necessary, and

would require approval by the federal testing authorities. Thus, the Secretary of State determined this requirement will not take effect until 3/31/2008. The Secretary of State implemented all other recommendations at the current time.

6. Software Coding Standards. The expert panel recommended using software hardening standards similar to standards implemented by either NSA or NIST requirements. The panel recommended that these requirements include standards for at least: input validations, range errors, API abuses, Time and State conditions, code quality conditions, and encapsulation conditions.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(f). The Secretary of State gave careful consideration to the forthcoming VVSG requirements that may duplicate the requirements listed here; however the coding restrictions more closely define parameters for the source code evaluation and were included in the requirements for that reason.

7. Removable Media Security. The expert panel recommended that security controls on removable storage media include authentication and validation of stored data through standard cryptography requirements as identified in documents such as Federal Information Processing Standards (FIPS) 140, and FIPS 180. Additionally, the panel recommended requiring virus scan software to operate on any workstation and/or server where removable media could be inserted.

   - The Secretary of State implemented these recommendations in section 45.5.2.6.1(g).

8. Telecommunication Security. The expert panel recommended that telecommunications devices be restricted as much as possible given the threat potential of public networks, provided hardening requirements for modems to include cryptography verification to FIPS 180 standards, requested wireless communications be completely restricted, and that audit capabilities be required for any transmission stream.

   - The Secretary of State implemented the recommendation of the expert panel in section 45.5.2.7 of Rule 45, 8 CCR 1505-1. In addition to this, the Secretary of State also mitigates these concerns through county security procedures.

D. Procedural Changes

The expert panel encouraged the Secretary of State to reconsider previous practices to modify and enhance the evaluation and documentation process of work product through the certification process.

1. VSTL Review Process. The expert panel suggested that the Secretary of State review all VSTL documents for compliance with federal standards. Individual reports may only contain a picture of the devices that were tested, and multiple reports may be required for a full picture of the VSTL Testing process. In addition, the panel recommended that the Secretary of State review not just the

test reports, but also the test logs, technical data packages and require that vendors consent to the Secretary of State discussing any questions or concerns regarding the VSTL testing with the VSTL testers. The goal is not to determine if the VSTL properly conducted the test, but instead to determine whether the VSTL conducted the test as required, drew a conclusion on the results of the test and made recommendations to the EAC for certification. If the federally mandated tests are not completed, then the Secretary of State will send the system back to the VSTL/EAC for re-testing of that specific component.

- The Secretary of State implemented this into Rule 45, 8 CCR 1505-1 for certification in section 45.5.2.4.2.

2. Chain of Evidence. The expert panel suggested that the Secretary of State adopt federal guidelines for the establishment and distribution of a trusted build version of a voting system used for testing. Having the capability to test the same build version of the software that VSTL labs are using for testing is imperative to maintaining the public confidence in DREs. Additionally, the State should research and consider methods other states have used in distributing and maintaining the chain of evidence of the software from the federal level down to the county level.

   - The Secretary of State implemented this procedure into Rule 45, 8 CCR 1505-1, and additionally has implemented models similar to those used in Maryland and Georgia for physically observing and documenting the chain of evidence for the trusted build being distributed to each device used in the State.

3. Documentation of Testing. The expert panel suggested that a detailed test log be developed including specific sections to document test scripts used, test environment, expected outcome, mitigating controls, test numbers, and a section for observations, notes and document attachments. Additionally, the expert panel recommended that the Secretary of State video document both the certification process and the implementation of the trusted build.

   - The Secretary of State implemented these recommendations and has revised the test log to reflect the suggestions, and has developed a strategy for adding video documentation of certification testing and trusted build installation.

Review of Public Comments

The Secretary of State evaluated and determined which public comments to adopt, modify or accept based on the overall direction of Rule 45, 8 CCR 1505-1. With respect to public comments, the Secretary of States' findings with input from the expert panel fell into one of the following four categories:

1. <u>Already Addressed</u>

The drafting and notice process evolved over the course of three months and various drafts were released to the public. The first draft released identified many areas that included items that "needed development" which would be coming at a later time. Many

of the initial comments received were addressed by the panel during the various drafting meetings held. Some examples of the submissions:

- "We feel there is no method by which to test a voter friendly system (45.5.2.3.2) and this will be lead to subjective judgment by the State staff." Consistent with the expert panel's recommendation, this item was removed by the Secretary of State.
- "The types of standards being discussed are not even in the draft of VVSG 2007 and are still under debate in some cases (like EAL-4)." Initially, the expert panel recommended this requirement, but later withdrew this recommendation because the standards are not yet defined and therefore cannot be evaluated or enforced. The Secretary of State removed the requirement from the draft versions of the rule.
- "Rule 45.11.5 allows a jurisdiction to opt out of acceptance testing of machines if they choose which is inconsistent with the other portions of the rule." The expert panel had recommended mandatory acceptance testing, which was implemented by the Secretary of State.

2. Implemented with Modifications

Based on the technical nature of the requirements and specific direction that the expert panel gave to drive the process, there were instances where the panel had to modify an initial suggestion to ensure consistency. Some examples of this in the submissions are:

- "This [45.6.2.3.3] should indicate that it includes a recall question and successor that counts the successor vote only if a choice has been selected on the recall question." The expert panel recommended the Secretary of State, the addition of the recall question in the requirement. The Secretary of State added the requirement for testing, but deferred to C.R.S. Title 1 for the specifics on handling the detail of the recall question and suggested adding the requirements to the functional testing procedures. This process is understood as the normal method for rule-making by the Secretary of State's office so that in the event a statute changes, the rule will not be invalidated.
- "A closed network must provide no communications path to the outside world." The expert panel recommended tightening the definition of a closed network to be consistent with their other recommendations on security standards in relation to networks. The panel agreed with the Secretary of State's requirements that with the combination of the new definition of closed network and the telecommunications devices hardening requirements provided in 45.5.2.7, that the environment is secured.
- "This would have to be done electronically [45.5.2.9.24]; I see no feasible way to get a paper printout to include/exclude races unless it was fed through some type of pre-programmed tabulator system." The Secretary of State changed the wording of the requirement be clarified to allow an elections administrator to properly identify provisional ballots recorded on V-VPAT paper.

3. Clarified Intention in Rule

In both the public comments received and internal meetings, certain language inconsistencies (SOS vs. Secretary of State for example) and unclear issues were raised, requiring clarification. Examples are :

- "In section 45.5.2.3.19 does the Secretary really want to test for fungus growth as required in the Guideline Four of the MIL HDBK 454?" The expert panel recommended this requirement only apply with respect to the handbook's requirements for parts and materials. The Secretary of State modified the requirement for clarity.
- "How is a system supposed to log a hardware reset [45.5.2.5.3]?" The Secretary of State clarified the requirement to apply to hardware initialization.
- "Do they [requirements] apply equally to the ballot definition system, the reporting system, the DRE as well as the optical scan [45.5.2.6.1(a)]?" The expert panel evaluated requirements and made recommendations to clarify instances where specific components should be referenced versus the broader "voting system" reference when all components should be addressed. The Secretary of State modified the requirements per the recommendations.
- "Is 'user' here [45.5.2.8.2(i)] defined as the voter?" The expert panel reviewed the entire document searching for terms such as user, voter, and operator, and recommended clarifications particular to those references, which were implemented by the Secretary of State.
- "Very detailed software structuring requirements should not be codified in Colorado statutes or regulations like this. Instead there should be good security evaluations against more established criteria." The expert panel re-evaluated the requirements for source code review, independent testing, operating system hardening, and software coding constructs. The experts recommended industry standard requirements from NIST, the NSA, or in the case of the software coding requirements, directly from the language of the VVSG.

4. Not Implemented

In some cases, public comments and suggestions could not be adopted either due to the limited scope of Rule 45, 8 CCR 1505-1, inconsistencies with the general direction previously recommended by the expert panel, or because the Secretary of State did not have statutory authority to adopt such suggestions. Some examples of this are:

- "Improve Logic and Accuracy test and equipment acceptance test procedures." This suggestion would require modification to Rule 11, 8 CCR 1505-1, which is not in the scope of Rule 45 and certification testing. The rule for certification testing does ensure certification tests are conducted in "election mode" only (45.6.2.3.2).
- "Election results should not be revealed publicly until at least 24 hours after the close of polls." This suggestion is not within the scope of certification testing and should be addressed with the Colorado Legislature.
- "The rule does not require compliance with the new standard [2005 VVSG] but instead provides that vendors only need to document their plans to comply with the requirement – a whole year later." The Secretary of State may not incorporate standards into a rule that are not yet in place (C.R.S. 24-4-103 (12.5)(a)). The 2005 VVSG becomes effective in December of 2007. The expert panel recommended that the rule be re-evaluated after that time. However, the expert panel studied the 2005 VVSG to determine if it should recommend that any of those requirements be adopted by Colorado now. In several instances, the experts recommended and the

Secretary of State adopted recommendations to include some of those requirements in the present rule changes, including: password requirements, the trusted build model, software design controls, database hardening, and source code review.

- "There are standards organizations working on Electronic Data Interchange standards, specifically the IEEE [45.5.2.1.7]. Reference should be added that with the proclamation of such standards, the standards will be adopted by the State." As stated earlier, the Secretary of State may not incorporate standards that are not yet in place (C.R.S. 24-4-103(12.5)(a)). Nonetheless, the expert panel reviewed some of the documents by the IEEE and recommended that the existing requirement remain as written for data transfers.
- "If the systems applying for certification… are approved and certified by the EAC why use valuable state resources to evaluate those previously tested requirements and components[45.5.2.4.2]?" The expert panel recommended that the Secretary of State review the documentation submitted to determine that the system meets or exceeds federal qualifications and not duplicate efforts by the testing authorities and federal authorities. This was recommended due to prior instances where required federal tests were not completed, or not completed satisfactorily, which may impact State-level testing.

2. Statutory Authority

Amendments and revisions to the Colorado Secretary of State Election Rules are adopted pursuant to the following statutory provisions:

1. Section 1-1-107(2)(a), C.R.S. (2006), which authorizes the Secretary of State:

"[t]o promulgate, publish, and distribute . . . such rules as the secretary of state finds necessary for the proper administration and enforcement of the election laws."

2. Section 1-1.5-104(1), C.R.S. (2006), which provides that:

"The secretary may exercise such powers and perform such duties as reasonably necessary to ensure that the state is compliant with all requirements imposed upon it pursuant to HAVA . . . including, without limitation, the power and duty to:

(e) Promulgate rules in accordance with the requirements of article 4 of title 24, C.R.S., as the secretary finds necessary for the proper administration, implementation, and enforcement of HAVA and of this article."

3. Section 1-5-616(1), C.R.S. (2006), which states:

"The secretary of state shall adopt ruled in accordance with article 4 of title 24, C.R.S. that establish minimum standards for electronic and electromechanical voting systems regarding:

(g) Security Requirements"

References

Feldman, Ariel, Halderman, Alex, Felten, Edward (2006). *Security Analysis of the Diebold AccuVote-TS Voting Machine.* Center for Information Technology Policy and Department of Computer Science, Princeton University.

Hursti, Harri (2005). *The Black Box Report. Security Alert: July 4, 2005. Critical Security Issues with Diebold Optical Scan Design.* Black Box Voting.

Hursti, Harri (2006). *Diebold TSx Evaluation. Security Alert: May 11, 2006. Crtitical Security Issues with Diebold TSx*. Black Box Voting.

Kiayias, A., Michel, L., Russell, A., Shvartsman, A.A. (2006). *Security Assessment of the Diebold Optical Scan Voting Terminal.* UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut.

Kohno, Tadayoshi, Stubblefield, Adam, Rubin, Aviel, Wallach, Dan (2004). *Analysis of an Electronic Voting System*. John Hopkins University, Information Security Institute; Department of Computer Science, Rice University; Department of Computer Science and Engineering, University of California at San Diego.

Norden, Lawrence (2006). *Voting System Security, Accessibility, Usability, and Cost.* The Brennan Center For Justice Voting Technology Assessment Project.

25.3.7.1 The electronic transmission log as well as any other ETS or fax records shall be maintained as part of the official election record.

26.2 Emergency Registration and use of Provisional Ballots in the County Clerk and Recorder's Office

26.2.1 If the elector applies for an emergency registration that cannot be qualified in the clerk's office at the time of the registration pursuant to section 1-2-217.5(4), C.R.S., the elector shall be issued a provisional ballot. The elector's registration must be confirmed by the designated election official at the time that the provisional ballots are verified or the provisional ballot shall not be counted.

26.2.2 If an elector whose name is not in the registration records, appears in person at the county clerk and recorder's office and states that he or she has timely registered through an agency pursuant to section 1-2-504, C.R.S., can affirm to the name, location of, and approximate date he or she completed the application at the agency or provide an application receipt, and provides an ID as defined in section 1-1-104(19.5), C.R.S., the elector shall be offered emergency registration and be offered a regular ballot.

26.2.2.1 If the elector does not provide an ID the elector shall be offered a provisional ballot. The county clerk and recorder shall note on the provisional ballot envelope that the elector did not have an ID.

26.2.2.2 If the elector is able to produce an application receipt from the agency registration, but does not provide an ID pursuant to section 1-1-104(19.5), C.R.S., the elector shall surrender the receipt to the election judge, and the county clerk and recorder shall attach the receipt to the provisional ballot envelope.

26.2.3 If an elector whose name is not in the registration records, appears in person at the county clerk and recorder's office and states that he or she has timely registered through a Voter Registration Drive ("VRD") pursuant to section 1-2-504, C.R.S., can affirm to the name, location of, and approximate date he or she completed the application with the VRD or provide an application receipt, and provides an ID as defined in section 1-1-104(19.5), C.R.S., the elector shall be offered emergency registration and be offered a regular ballot.

26.2.3.1 If the elector does not provide an ID the elector shall be offered a provisional ballot. The county clerk and recorder shall note on the provisional ballot envelope that the elector did not have an ID.

26.2.3.2 If the elector is able to produce an application receipt from the VRD registration, but does not provide an ID pursuant to section 1-1-104(19.5), C.R.S., the elector shall surrender the receipt to the election judge, and the county clerk and recorder shall attach the receipt to the provisional ballot envelope.

26.2.4 If the elector's eligibility to vote cannot be verified, the provisional ballot shall not count, but

may constitute a registration for future elections.

30.3 Voter Registration by Mail

30.3.1 Registering by Mail. (Including Voter Registration Drives).

(a) The voter must provide one of the following identification numbers:

(b) The person's Colorado Driver's License number or ID number issued by the Department of Revenue; if the voter does not have a current and valid Colorado Driver's License or ID card issued by the Department of Revenue, the voter shall provide the last four digits of the voter's social security number.

(c) If a voter has not been issued a Colorado Driver's License number, ID card issued by the Department of Revenue or a Social Security card, the voter must provide a copy of one of the forms of identification listed in 30.1.6.

Authority: Sections 1-2-501(2)(a), C.R.S. and 1-1-104(19.5), C.R.S.

38.10 Prior to January 1, 2008, election judges shall make one certificate for each Vote Center in the form required by section 1-7-601, C.R.S.

38.12 After January 1, 2008, reconciliation shall consist of race-by-race comparison by precinct of the received tabulation to a tabulation report produced from the original tabulations sent from the precinct to those received at the Vote Center. All tabulation reconciliations must be accomplished prior to canvassing board certification of final results and shall be certified by the canvassing board. This certification of reconciliation shall be filed with the Secretary of State at the time the canvassing board certification of official election results is filed.

Rule 45. Rules Concerning Voting System Standards for Certification

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

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

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

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

45.1.4 "Ballot style assignment" means the creation of unique, specific ballots for an election 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 based on their

individual precincts.

45.1.5 “Closed network” means a network structure where devices are not connected to the internet or other office automation networks, except as allowable under section 45.5.2.7.

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

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

45.1.8 “EAC” means the United States Elections Assistance Commission.

45.1.9 “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.

45.1.10 “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.

45.1.11 “FEC” means the Federal Election Commission.

45.1.12 “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.

45.1.13 “Removable Storage Media” means any device that is intended to be removed that has the ability of storing or processing data for a voting system.

45.1.14 “Security” means the ability of a voting system to protect election information and election system resources with respect to confidentiality, integrity, and availability.

45.1.15 “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.

45.1.16 “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 such as: photographs, written notes, video and/or audio recorded notes.

45.1.17 “Trusted Build” means the write-once installation disk or disks for software and firmware for

which the Secretary of State or his/her agent has established the chain of evidence to the building of a disk, which is then used to establish and/or re-establish the chain of custody of any component of the voting system which contains firmware or software. The trusted build is the origin of the chain of evidence for any software and firmware component of the voting system.

45.1.18 "VSTL" means a voting system testing laboratory that provides engineering, testing, or evaluation services for voting systems, and is qualified by the EAC to conduct qualification testing on a 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.

45.2.1.2 Sufficient components shall be assembled to create a configuration that shall allow the system as a whole to meet the requirements as 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.

45.3 Certification Process Overview and Timeline

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

45.3.2 For a voting system to pass certification the voting system provider shall successfully complete all phases of the certification process which shall include: submitting a complete application; review of the documentation to evaluate if the system meets the requirements of this rule; demonstration of the system; and functional testing of the voting system which shall demonstrate substantial compliance with the requirements of this rule, Colorado Election Code, and any additional testing that is deemed necessary by the Secretary of State.

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

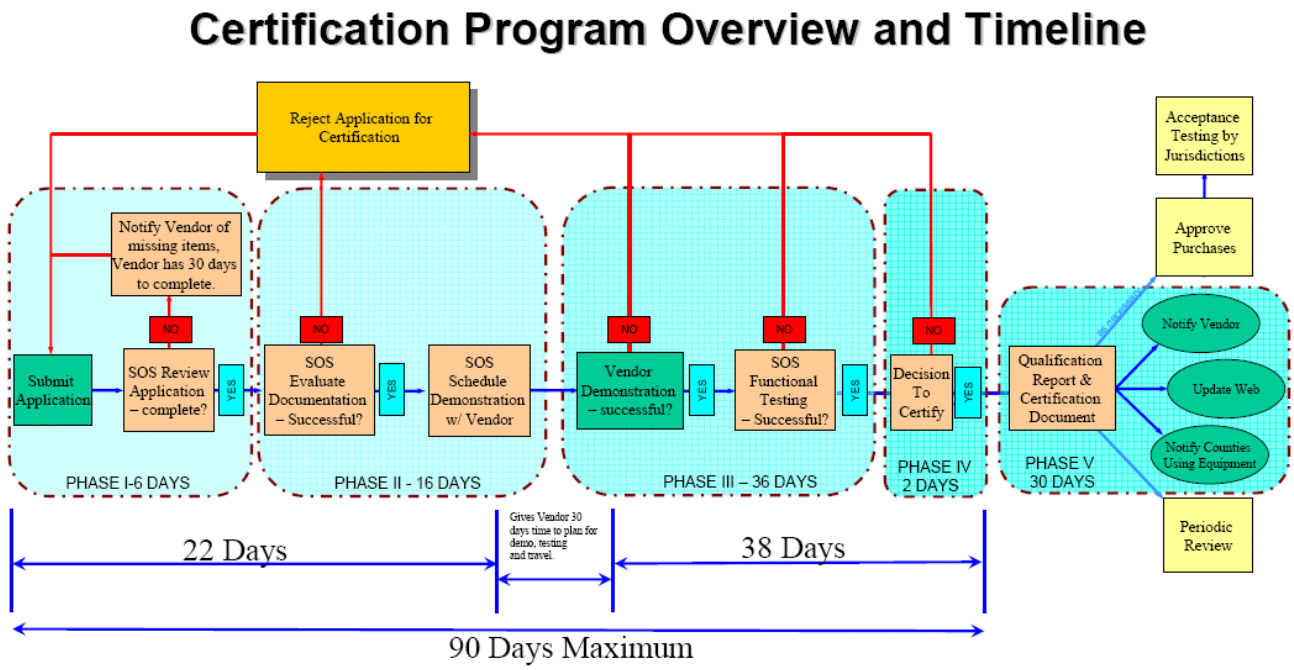
(a) Phase I – 6 days maximum. Voting system provider submits application and Secretary of State reviews for completeness. Voting system provider shall have 30 days to remedy and make application complete.

(b) Phase II – 16 Days maximum. Secretary of State reviews the documentation submitted and upon successful completion makes arrangements with voting system provider for demonstration.

(c) Phase III – 36 days maximum. When demonstration is complete, Secretary of State performs the functional testing.

(d) Phase IV – 2 days maximum. Upon completion of functional testing, Secretary of State makes a decision to cerfity a voting system and produces applicable certification document.

(e) Phase V – 30 days maximum. Upon decision to certify a voting system, Secretary of State shall produce a qualification report for the voting system and components certified, which shall be posted on the Secretary of State website.



45.4 Application Procedure

45.4.1 Any voting system provider may apply to the Secretary of State for certification at any time.

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

45.4.3 The voting system provider shall establish an escrow account pursuant to State procurement processes to compensate the Secretary of State for necessary outside costs associated with the testing of the system. The Secretary of State shall provide an estimate of costs for certification testing at the conclusion of Phase II evaluation.

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

45.4.5 Electronic copies of documentation are preferred and shall be submitted in lieu of a hard copy when possible.

45.4.6 If the EAC has established a trusted build for the system submitted for certification, the trusted build shall be provided by the EAC. The voting system provider shall execute and submit to the EAC any necessary releases for the EAC to provide the same, and shall provide the Secretary of State's office with a copy of such executed releases. The voting system provider shall pay directly to the EAC any cost associated with same. In addition, the voting system provider shall submit all documentation and instructions necessary for the creation of and guided installation of files contained in the trusted build which will be created at the start of functional testing and will be the model tested against. The Secretary of State reserves the right to add additional instructions or guidance for the use of the trusted build when initiating the chain of custody process for a jurisdiction using the specified equipment.

45.4.7 If the EAC does not have a trusted build for the voting system submitted for certification, the voting system provider shall coordinate with the Secretary of State for the establishment of the trusted build. At a minimum this shall include a compilation of files placed on write-once media for which the Secretary of State has observed the chain of evidence from time of source code compliation through delivery, and an established hash file distributed from a VSTL or the National Software Reference Library to compare federally certified versions against. All or any part of the Trusted Build disks may be encrypted. They should all be labeled as Proprietary Information if applicable and with identification of the voting system provider's name and release version based on the voting system provider's release instructions.

45.4.8 All materials submitted to the Secretary of State shall remain in the custody of the Secretary of State during the life of the certification and for twenty-five (25) months after the last election in which the system is used with the exception of any equipment provided by the voting system provider to purposes of testing.

45.4.9 In addition to the application and the documentation specified above, the Secretary of State may request additional information from the applicant, as deemed necessary by the Secretary of State.

45.5 Voting System Standards

45.5.1 Federal Standards

45.5.1.1 All voting systems shall meet the voting systems standards pursuant to section 1-5-601.5, C.R.S., and Secretary of State Rule 37.3.

45.5.1.2 All voting system software, hardware, and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not 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 Secretary of State or his/her designee shall review all of the documentation submitted from federal testing for compliance with applicable laws and regulations. Documentation of tests completed at the federal level may be used for compliance of duplicate State level requirements; however compliance with federal standards does not necessarily establish compliance with Colorado standards.

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:

(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 accurately integrate election day voting results with absentee, early voting and provisional ballot results.

45.5.2.1.4 The voting system shall be able to count all of an elector's votes on a provisional ballot or only federal and statewide offices and statewide ballot issues and questions, as provided under section 1-8.5-108(2), C.R.S.

45.5.2.1.5 The voting system shall provide for the tabulation of votes cast in split precincts where all voters residing in one precinct are not voting the same ballot style.

45.5.2.1.6 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 application shall provide authorized users with the capability to produce electronic files including election results in either ASCII (both comma-delimited and fixed-width) or web-based format that shall contain (a) all data or (b) any user selected data elements from the database. The software shall provide authorized users with the ability to generate these files on an "on-demand" basis. After creating such files, the authorized users shall, at their discretion, have the capability to copy the files to diskette, tape, or CD-ROM or to transmit the files to another information system.

(a) Exports necessary for the Secretary of State shall conform to an agreed upon format.

(b) Export files shall be generated so that election results can be communicated to the Secretary of State on election night both during the accumulation of results and after all results have been accumulated.

45.5.2.1.8 The voting system shall include hardware and software to enable the closing of the remote 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 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 which shall 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 or questions; and

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

(d) Abstract shall include an election judge's certificate and statement that contains:

(i) 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; and

(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) Ability to produce multiple copies of the unofficial results at the close of the election.

(g) Ability to accommodate a two page ballot (races on four faces) is required.

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 voting system application shall ensure that an election setup may not be changed once ballots are printed and/or election media devices are downloaded for votes to be conducted without proper authorization and acknowledgement by the application administrative account. The application and database audit transaction logs shall accurately reflect the name of the system operator making the change(s), the date and time of the change(s), and the "old" and "new" values of the change(s).

45.5.2.2 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 during functional testing for certification. Speed requirements are based on a printed double sided complete 18" ballot with a minimum of 20 contests:

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

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

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

45.5.2.2.3 The voting system provider shall publish and specify processing standards for each component of the voting system as part of the documentation required for certification.

45.5.2.2.4 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 an evaluator of the software would have pauses equal to less than five (5) seconds 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 initial layout is less than 10 seconds per ballot style;

(b) Election Media Download for vote storage media without audio files is less than 35 seconds per media;

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

(d) The application software upon creation of the layout of the races on ballot shall produce the ballot image (on screen) for the evaluator in less than thirty (30) seconds per ballot image.

45.5.2.2.5 At no time shall third party hardware or software negatively impact performance levels of voting system application, 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. The voting system shall substantially comply with these requirements to be considered successful in the conduct of an election on the voting system.

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

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

(b) Non-Operating – Max. 140 Degrees Fahrenheit; Min. 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 system.

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

45.5.2.3.4 The Ballot Definition Subsystem shall be capable of formatting ballot styles in English and any alternate languages as are necessary to comply with The “Voting Rights Act of 1965” 42 U.S.C. § 1973c et seq. (1965).

45.5.2.3.5 The voting system application shall allow the operator to generate and maintain an administrative database containing the definitions and descriptions of political subdivisions and offices within the jurisdiction.

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

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

45.5.2.3.8 The ballot definition subsystem shall be capable of handling at least 500 potentially active voting positions, arranged to identify party affiliations in a primary election, offices and their associated labels and instructions, candidate names and their associated labels and instructions, and ballot issues or questions and their associated text and instructions.

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

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

45.5.2.3.11 The trusted build of the voting system software, installation programs, and third party software (such as operating systems, drivers, etc.) used to install or to be installed on voting system devices shall be distributed on a write-once media.

45.5.2.3.12 The voting system shall allow the system administrative account to verify that the software installed is the certified software by comparing it to the trusted build or other reference information.

45.5.2.3.13 All DRE voting devices shall use touch screen technology or other technology providing visual ballot display and selection. The voting system provider shall provide documentation concerning the use of

touch screen or other display and selection technology, including but not limited to:

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

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

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

(d) Any available data on problems caused for persons who experience epileptic seizures due to the DRE voting devices' screen refresh rate.

45.5.2.3.14 The voting system shall contain a control subsystem that consists of the physical devices and software that accomplish and validate the following operations:

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

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

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

45.5.2.3.16 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.

45.5.2.3.17 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. Telecommunications 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 auditing and error check as required by 45.5.2.7.

45.5.2.3.18 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 meet or exceed MIL-HDBK-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 only as is relevant to this section.

45.5.2.3.19 All electronic 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 (3) hours the ability to:

(i) Continue to scan or image voters' ballots;

(ii) Tabulate accurately voters' choices from the ballots;

(iii) Store accurately 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 three (3) hours the ability to:

(i) Continue to present ballots accurately to voters;

(ii) Accept voters' choices accurately on the devices;

(iii) Tabulate voters' choices accurately;

(iv) Store voters' choices accurately in all storage locations on the device; and

(v) Transmit required results files accurately if power failure is experienced during transmittal of results.

(c) For V-VPAT devices connected to DREs, this capability shall include at a minimum for a period of not less than three (3) hours the ability to:

(i) Continue to print voters' choices on the DRE accurately and in a manner that is identical to the manner of the printers' operations during a period of normal electrical operations; and

(ii) Continue to store the printed ballots in a secure manner that is identical to the manner of the printers' operations during a period of normal electrical operations.

(d) The voting system provider shall deliver to the Secretary of State documentation detailing estimated time of 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 Secretary of State documentation specifying the steps and times required for charging batteries for each type of optical scanner, ballot imager, DRE and V-VPAT they provide.

45.5.2.3.20 The voting system provider's software application shall be able to recover operations after a power outage or other abnormal shutdown of the system on which that application and database are operating without loss of more than the current transaction data record on which the administrative account or authorized operator account is currently working.

45.5.2.3.21 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.

45.5.2.3.22 The voting system and all associated components shall have an estimated useful life of at least eight (8) years. Voting system provider shall provide documentation of the basis for the estimate.

45.5.2.3.23 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 other documentation requirements in this rule, the voting system provider shall provide the following documents:

(a) Standard Issue Users/Operator Manual;

(b) System Administrator's / Application Administration Manual;

(c) Training Manual (and materials);

(d) Systems Programming and Diagnostics Manuals; and

(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 VSTL qualification reports, test logs, and technical data packages shall be evaluated to determine if the voting system meets the requirements of this rule and have completed the applicable federal certification requirements at the time of State testing. Failure to provide such documentation of independent testing will result in the voting system application being rejected.

(a) The voting system provider shall execute and submit any necessary releases for the applicable VSTL and/or EAC to discuss any and all procedures and findings relevant to the voting system submitted for certification with the Secretary of State's office. The voting system provider shall provide a copy of the same to the Secretary of State's office.

45.5.2.4.3 As of March 31, 2008, any voting system provider submitting a voting system for certification shall, prior to applying for certification, have completed and provided documentation of an independent analysis of the system coordinated through the Secretary of State's office. The independent analysis shall include:

(a) Application penetration test conducted to OSSTMM 2.2 standards for White or Double Gray box testing;

(b) Source code evaluated to the requirements identified in 45.5.2.6.1(f);

(c) A complete review of the source code for these two tests shall be provided as part of the certification process;

(d) A complete report of acceptable compensating controls shall be provided with the tests conducted for items (a) and (b) of this section.

(i) Inability for the voting system provider to provide acceptable compensating controls will require a retest of the system under this section until all compensating controls have a valid procedural mitigation strategy.

(e) The vendor shall use an EAC approved VSTL to perform the independent analysis;

(f) The Secretary of State or the designated agent shall review all work performed by contractor for quality of work product under this section. The review may include any or all of the following requirements:

(i) Review of records at contractors' site;

(ii) Interviews of employees who performed the work; and

(iii) Interviews of any subcontractors used.

(g) The Secretary of State has the right to reject evaluations performed if not satisfied with the work product and may request additional reviews of the voting system provider.

45.5.2.4.4 Documentation submitted to the Secretary of State shall be reviewed to ensure the voting system has been tested to federal standards.

(a) Voting System providers shall provide the Secretary of State 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 audit logs of system operation and system operators actions which shall be substantially compliant to allow operations and input commands to be audited.

45.5.2.5.2 The voting systems shall include detailed documentation as to the level, location, and programming of audit trail information throughout the system. The audit information shall apply to:

(a) Operating Systems (workstation, server, and/or DRE);

(b) Election Programming Software;

(c) Election Tabulation devices – optical scan and DRE; and

(d) Election Result Consolidation and Reporting.

45.5.2.5.3 The voting system shall track and maintain audit information of the following voting system application 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), initialize devices, backup devices, and voting activity; and

(e) Hardware events – add hardware, remove hardware, initialize 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, logs, or reports.

45.5.2.5.5 Vote tabulation devices shall allow for an alternate method of transfer of audit records if the device or a memory storage device is damaged or destroyed.

45.5.2.5.6 All transaction audit records of the voting system application database shall be maintained in a file outside or separate from the database, which is not accessible by user/operator 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 and role based access control. The following requirements shall apply:

(i) The operating system Administrative Account shall not have access to read or write data to the database and shall not have the ability or knowledge of the database administrator password;

(ii) The operating system administrative account shall not be required to use any function of the voting system during normal operations;

(iii) A unique system user/operator 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; and

d. No access to modify other user accounts on the system.

(iv) A unique application administrative account shall be created which has full access and rights to the application and database;

(v) A unique application user/operator account shall be created with limited rights specifically designed to perform functional operation within the scope of the application. This user/operator shall be restricted in the creation or modification of any user/operator accounts; and

(vi) Voting system provider shall not have administrative account, or administrative account access.

(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) All components of the voting system shall include the limited use of non-routable IP address configurations for any device connected to the closed network. For the purposes of this requirement non-routable IP addresses are those defined in the RFC 1918 Address base; and

(iii) The voting system shall be tested to contain provisions for updating security patches, software and/or service packs without access to the open network.

(c) After March 31, 2008, all voting systems submitted for certification shall meet the following requirements for database security:

(i) All voting systems submitted for certification using Oracle 9i, Oracle 10g, or Microsoft SQL shall be

hardened to the existing and published NSA guidelines for databases as follows:

a. Oracle 9i and Oracle 10g databases shall be hardened to the Center for Internet Security Benchmark for Oracle 9i/10g Ver. 2.0;

b. Microsoft SQL databases shall be hardened to the NSA Guide to the Secure Configuration and Administration of Microsoft SQL Server 2000.

(ii) All other voting system databases submitted for certification shall have the voting systems databases hardened to database manufacturer's existing hardening requirements; or

(iii) If the manufacturer has not established requirements for the specifically designed system, the voting systems submitted for certification shall have the voting systems databases hardened to the voting system providers' specifications.

(iv) All voting systems submitted for certification shall have all voting systems databases restricted to allowing access to database authentication from application only (or through application only);

(v) All data stored at rest in any voting system database shall be encrypted in accordance with section (vi) of this requirement; and

(vi) All Cryptography modules shall be documented by the voting system provider to be certified to US Federal Information Processing Standard (FIPS-140-2), and validated to FIPS 180 standards.

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

(i) After March 31, 2008, all voting systems being submitted for certification shall have all operating systems hardened to NSA guidelines for operating systems as follows:

a. Apple max OS X systems shall be hardened to the NSA Apple Mac OS X v10.3.x "Panther" Security Configuration Guide Version 1.1;

b. Apple Server Operating Systems shall be hardened to the NSA Apple Mac OS X Server v10.3.x "Panther" Security Configuration Guide;

c. Microsoft Windows XP Operating systems shall be hardened to the NSA Windows XP Security

Guide Version: 2.2 and the NSA Windows XP Security Guide Addendum Version 1.0;

d. Microsoft Windows 2000 operating systems shall be hardened to the following NSA Guides:

i. Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0 Version 1.4;

ii. Guide to the Secure Configuration and Administration of Microsoft ISA Server 2000 Version 1.5;

iii. Guide to Securing Microsoft Windows 2000 Active Directory Version 1.0;

iv. Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services Version 2.1.1;

v. Guide to Securing Microsoft Windows 2000 DHCP Version 1.3;

vi. Guide to Securing Microsoft DNS Version 1.0;

vii. Guide to Securing Microsoft Windows 2000 Encrypting File System Version 1.0;

viii. Guide to Securing Microsoft Windows 2000 File and Disk Resources Version 1.0.1;

ix. Guide to securing Microsoft Windows 2000 Group Policy Version 1.1;

x. Group Policy Reference Version 1.0.8;

xi. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set Version 1.2.1;

xii. Microsoft Windows 2000 IPSec Guide Version 1.0;

xiii. Guide to Windows 2000 Kerberos Settings Version 1.1;

xiv. Microsoft Windows 2000 Network Architecture Guide Version 1.0;

xv. Microsoft Windows 2000 Router Configuration Guide Version 1.02;

xvi. Guide to Securing Microsoft Windows 2000 Schema Version 1.0;

xvii. Guide to Securing Microsoft Windows 2000 Terminal Services Version 1.0; and

xviii. Guide to Securing Windows NT/9x Clients in a Windows 2000 Network Version 1.0.2;

e. Microsoft Windows Server 2003 operating systems shall be hardened to the NSA Microsoft Windows Server 2003 Security Guide Version 2.1 and The Microsoft Windows Server 2003 Security Guide Addendum Version 1.0;

f. Sun Solaris 8 operating systems shall be hardened to the NSA Guide to the Secure Configuration of Solaris 8 Version 1.0; and

g. Sun Solaris 9 operating systems shall be hardened to the NSA Guide to the Secure Configuration of Solaris 9 Version 1.0.

(ii) All other voting system operating systems submitted for certification after March 31, 2008 shall have all operating systems hardened to existing manufacturer's hardening requirements; or

(iii) If the manufacturer has not established requirements for the specifically designed system, after March 31, 2008, all voting systems being submitted for certification shall have all operating systems hardened to the voting system providers' specifications;

(iv) The voting system provider shall provide documentation containing a list of minimum services and executables that are required to run the voting system application;

(v) The voting system provider shall configure the voting system operating system of the workstation and/or server used for the election management software to the following requirements:

a. The ability for the system to take an action upon inserting a removable media (Autorun) shall be disabled; and

b. The voting system shall only boot from the drive or device identified as the primary drive. The voting system shall not boot from any alternative device.

(vi) The voting system provider shall use a virus protection/prevention application on the election

management server(s) /workstations which shall be capable of manual updates without the use of the internet.

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

(i) All passwords shall be stored and used in a non-reversible format;

(ii) Passwords to database shall not be stored in database;

(iii) Password to database shall be owned and known only known by the application;

(iv) The application's database management system shall require separate passwords for the administrative account and each operator account with access to the application;

(v) The system shall be designed in such a way that the use of the administrative account password shall not be required for normal operating functions at any remote location;

(vi) The system shall be designed in 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; and

(viii) As of March 31, 2008 all voting systems submitted for certification shall have all components of voting system 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) As of March 31, 2008, all voting system software submitted for certification 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:

(i) Self-modifying, dynamically loaded or interpreted code is prohibited, except under the security provisions required by federal testing. 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; and

c. Dynamic memory allocation and management.

(ii) By March 31, 2008, all voting systems submitted for certification shall have application software designed in a modular fashion. 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. All modules shall be designed in accordance with the following requirements for systems submitted for certification after March 31, 2008:

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. 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 shall 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 shall explicitly protect all recorded votes and audit log information and shall implement formal exception handlers provided by the language.

e. Process flow within the modules shall be restricted to combinations of the control structures defined below. This shall 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.

    i. In the constructs, any ‘process’ may be replaced by a simple statement, a subroutine or function call, or any of the control constructs.

    ii. Using the replacement rule to replace one or both of the processes in the Sequence construct with other Sequence constructs, a large block of sequential code may be formed. The entire chain is recognized as a Sequence construct and is sometimes called a BLOCK construct. Sequences shall be marked with special symbols or punctuation to delimit where it starts and where it ends.

    iii. A special case of the GENERAL LOOP is the FOR loop. The FOR loop may be programmed as a DO-WHILE loop. The FOR loop shall execute on a counter. The control FOR statement shall define a counter variable or variables, a test for ending the loop, and a standard method of changing the variable(s) on each pass such as incrementing or decrementing.

    iv. The use of the FOR loop shall avoid common errors such as a loop that never ends. The

GENERAL LOOP shall not be used where one of the other loop structures will serve. However, if defined in the language, it may be useful in defining some loops where the exit needs to occur in the middle. Also, in other languages the GENERAL LOOP logic may be used to simulate the other control constructs. The use of the GENERAL LOOP shall require the strict enforcement of coding conventions to avoid problems.

v. The voting system software code shall use uniform calling sequences. All parameters shall either be validated for type and range on entry into each unit or the unit comments shall explicitly identify the type and range for the reference of the programmer and tester. Validation may be performed implicitly by the compiler or explicitly by the programmer.

vi. The voting system software code shall have the return explicitly defined for callable units such as functions or procedures (do not drop through by default) for C-based languages and others to which this applies, and in the case of functions, shall have the return value explicitly assigned. Where the return is only expected to return a successful value, the C convention of returning zero shall be used. If an uncorrected error occurs so the unit shall return without correctly completing its objective, a non-zero return value shall be given even if there is no expectation of testing the return. An exception may be made where the return value of the function has a data range including zero.

vii. The voting system software code shall not use macros that contain returns or pass control beyond the next statement.

viii. For those languages with unbound arrays, the voting system software shall provide controls to prevent writing beyond the array, string, or buffer boundaries.

ix. For those languages with pointers or which provide for specifying absolute memory locations, the voting system software shall provide controls that prevent the pointer or address from being used to overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored.

x. For those languages supporting case statements, the voting system software shall have a default choice explicitly defined to catch values not included in the case list.

xi. The voting system software shall provide controls to prevent any vote counter from overflowing. An assumption that the counter size is large enough such that the value will never be reached does not meet this requirement.

xii. The voting system software code shall be indented consistently and clearly to indicate logical levels.

xiii. Excluding code generated by commercial code generators, the voting system software code is written in small and easily identifiable modules, with no more than 50% of all modules exceeding 60 lines in length, no more than 5% of all modules exceeding 120 lines in length, and no modules exceeding 240 lines in length. “Lines” in this context, are defined as executable statements or flow control statements with suitable formatting and comments.

xiv. Where code generators are used, the voting system software source file segments provided by the code generators shall be marked as such with comments defining the logic invoked and, a copy of the source code provided to the accredited test lab with the generated source code replaced with an unexpanded macro call or its equivalent.

xv. The voting system software shall have no line of code exceeding 80 columns in width (including comments and tab expansions) without justification.

xvi. The voting system software shall contain no more than one executable statement and no more than one flow control statement for each line of source code.

xvii. In languages where embedded executable statements are permitted in conditional expressions, the single embedded statement may be considered a part of the conditional expression. Any additional executable statements should be split out to other lines.

xviii. The voting system software shall avoid mixed-mode operations. If mixed mode

usage is necessary, then all uses shall be identified and clearly explained by comments.

xix. Upon exit() at any point, the voting system software shall present a message to the operator indicating the reason for the exit().

xx. The voting system software shall use separate and consistent formats to distinguish between normal status and error or exception messages. All messages shall be self-explanatory and shall not require the operator to perform any look-up to interpret them, except for error messages that require resolution by a trained technician.

xxi. The voting system software shall reference variables by fewer than five levels of indirection.

xxii. The voting system software shall have functions with fewer than six levels of indented scope, counted as follows:

```
int function()
{
        if (a = true)
1       {
                if ( b = true )
2               {
                        if ( c = true )
3                       {
                                if ( d = true )
4                               {

        while(e > 0 )
5                                       {

        code

        }
}
}
}
}
}
```

xxiii. The voting system software shall initialize every variable upon declaration where permitted.

xxiv. The voting system software shall have all constants other than 0 and 1 defined or enumerated, or shall have a comment which clearly explains what each constant means in the context of its use. Where “0”

and “1” have multiple meanings in the code unit, even they shall be identified.

xxv. The voting system software shall only contain the minimum implementation of the “a = b ? c : d” syntax. Expansions such as “j=a?(b?c:d):e;” are prohibited.

xxvi. The voting system software shall have all assert() statements coded such that they are absent from a production compilation. Such coding may be implemented by ifdef()s that remove them from or include them in the compilation. If implemented, the initial program identification in setup should identify that assert() is enabled and active as a test version.

f. Control Constructs within the modules shall be limited to the acceptable constructs of 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 voting system provider 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 may nonetheless contain procedures (such as “methods” in object-oriented languages). In these programming languages, the procedures shall execute through these control constructs or their equivalents, as defined and provided by the voting system provider.

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.

g. All modules of the voting system software shall use the following naming conventions:

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

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

iii. 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 shall always be unique where modules are shared.

iv. 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.

h. All modules of the voting system software shall adhere to basic coding conventions. The voting system providers shall identify the published, reviewed, and industry-accepted coding conventions used.

i. All modules of the voting system software shall use the following comment conventions:

i. 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:

1. The purpose of the unit and how it works;

2. Other units called and the calling sequence;

3. A description of input parameters and outputs;

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

5. Global variables used; and

6. Date of creation and a revision record.

ii. 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.

iii. In-line comments shall be provided to facilitate interpretation of functional operations, tests, and branching.

iv. Assembly code shall contain descriptive and informative comments such that its executable lines can be clearly understood.

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

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

i. If software is resident in the system as firmware, the voting system provider shall 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.

ii. 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 shall provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.

iii. The voting system bootstrap, monitor, and device-controller software may be resident permanently as firmware, provided that this firmware has been shown to be inaccessible to activation or control by any means other than by the authorized initiation and

execution of the vote counting program, and its associated exception handlers.

iv. The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.

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

vi. Independent analysis will test for the following conditions and report on absence or presence of the following input validations in accordance with section 45.5.2.4.3:

1. Path manipulation;

2. Cross Site Scripting.Basic X;

3. Resource Injection;

4. OS Command Injection (also called “Shell Injection”); and

5. SQL Injection.

vii. Independent analysis will test for the following conditions and report on absence or presence of the following range errors in accordance with section 45.5.2.4.3:

1. Stack Overflow;

2. Heap Overflow;

3. Format string vulnerability; and

4. Improper Null Termination.

viii. Independent analysis will test for following conditions and report on absence or presence of the following API abuses in accordance with section 45.5.2.4.3:

1. Heap Inspection; and

2. String Management/ Manipulation.

ix. Independent analysis will test for following conditions and report on absence or presence of the following Time and State

conditions in accordance with section 45.5.2.4.3:

1. Time-of-check/Time-of-use race condition; and

2. Unchecked Error Condition.

x. Independent analysis will test for following conditions and report on absence or presence of the following code quality conditions accordance with section 45.5.2.4.3:

1. Memory Leaks;

2. Unrestricted Critical Resource Lock;

3. Double Free;

4 Use After Free;

5. Uninitialized variable;

6. Unintentional pointer scaling;

7. Improper pointer subtraction; and

8. Null Dereference.

xi. Independent analysis will test for following conditions and report on absence or presence of the following encapsulation conditions in accordance with section 45.5.2.4.3:

1. Private Array-Typed Field Returned from a Public Method;

2. Public Data Assigned to Private Array-Typed Field;

3. Overflow of static internal buffer; and

4. Leftover Debug Code.

xii. The Application shall not open database tables for direct editing.

k. As of March 31, 2008, the voting system submitted for certification shall meet the following minimum requirements for removable storage media with data controls:

i. All voting data stored which includes vote records, ballot images, tally data and cast votes shall be authenticated and validated in accordance with cryptography requirements of subsection (c)(vii) of this requirement;

ii. All non-voting data stored shall be authenticated, encrypted, and validated in accordance with cryptography requirements of subsection (c)(vii) of this requirement; and

iii. Antivirus software shall be present and scan removable media upon insertion of media or media device on server and/or workstations hosting the elections management software.

45.5.2.6.2 The voting system provider shall provide documentation detailing voting system security in the areas listed below. The system shall contain documented configurations, properties and procedures to prevent, detect and log changes to system capabilities for:

(a) Defining ballot formats;

(b) Casting and recording votes;

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

(d) Reporting vote totals;

(e) Altering of voting system audit records;

(f) Changing, or preventing the recording of, a vote;

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

(h) Changing calculated vote totals;

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

(j) Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

45.5.2.6.3 The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing:

(a) Software access controls;

(b) Hardware access controls;

(c) Data communications;

(d) Effective password management;

(e) Protection abilities of a particular operating system;

(f) General characteristics of supervisory access privileges;

(g) Segregation of duties; and

(h) Any additional relevant characteristics.

45.5.2.6.4 The voting system shall include detailed documentation 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 jurisdictions that purchase the voting system.

45.5.2.7 Telecommunications Requirements

45.5.2.7.1 Telecommunications includes all components of the system that transmit data outside of the closed network as defined in this Rule.

45.5.2.7.2 All electronic transmissions from a voting system shall meet the following minimum standards:

(a) Modems from remote devices shall be “dial only” and cannot be programmed to receive a call;

(b) All communications of data in transfer shall be encrypted, authenticated and verified to the FIPS 140-2 standard and verified to the FIPS 180 standard; and

45.5.2.7.3 Any modem in any component failing to meet these criteria shall not be used by any voting system.

45.5.2.7.4 All wireless components on voting systems shall be disabled with the exception of line of sight infrared technology used in a closed environment where the transmission and reception is shielded from external infrared signals and can only accept infrared signals generated from within the system.

45.5.2.7.5 All systems that transmit data over public telecommunications networks shall maintain a clear audit trail that can be provided to the Secretary of State when election results are transmitted by telephone, microwave or any other type of electronic communication.

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

45.5.2.7.7 Any voting system provider of systems that cast individual ballots over a public telecommunications network shall provide detailed descriptions of:

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

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

45.5.2.7.8 In any situation in which the voting system provider's system transmits data through any telecommunications medium, the system shall be able to recover, either automatically or with manual intervention, from incomplete or failed transmission sessions and resume transmissions automatically when telecommunications are re-established.

(a) Recovery of transmissions shall include notations of the interrupted transmission session and the resumed transmission session in the system and application transaction logs.

(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.

45.5.2.7.9 Voting systems that use public telecommunications networks shall provide system documentation that clearly identifies all COTS hardware and software products and communications services used in the development and/or operation of the voting system, including operating systems, communications routers, modem drivers and dial-up networking software. Documentation shall identify the name, voting system provider, and version used for each such component.

45.5.2.7.10 Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

(a) Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components;

(b) Evaluate the threats and, if any, proposed responses.

(c) Develop responsive updates to the system and/or corrective procedures; and

(d) As part of certification requirements of the proposed system, provide assistance to customers, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the Secretary of State.

45.5.2.8 Accessibility Requirements

45.5.2.8.1 Specific minimum accessibility requirements include those specified in section 1-5-704 C.R.S., Secretary of State 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:

(i) The voting system shall allow the voter to pause and resume the audio presentation.

(ii) 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;

(d) All Touchscreen technology shall be tested for use of fingers as well as non-human touch that is both wet and dry;

(e) Voting systems shall include at least the ability to activate and navigate by means of push buttons, dials, wheels, keypads, and/or touch screens. By March 31, 2008, voting systems submitted for certification shall also include any form of either switches, sip and puff devices, or additional blink control devices; and

(f) Adjustability of color settings, screen contrasts and/or screen angles/tilt may be made by either the poll worker or voter if the system uses a display screen. A minimum of two color settings, two contrast settings and two angles shall be available for all display screens.

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;

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

(i) Method for adjusting 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 examined for certification by the Secretary of State. Any retrofitted voting system shall comply with the process and application for certification as identified by this rule.

45.5.2.9.3 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; and

(d) These devices may be integrated as appropriate to their operation.

45.5.2.9.4 V-VPAT devices shall allow voters to verify his or her selections on a paper record prior to casting ballots. The voter shall either accept or reject the choices represented on the paper record. Both the electronic record and the paper record shall be stored and retained 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 non-printer related services.

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 seventy-five (75) ballots cast without requiring the paper supply source, ink or toner supply, or any other similar consumable supply to be changed, assuming a fully printed double sided eighteen (18) inch ballot with a minimum of 20 contests.

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

45.5.2.9.17 As of March 31, 2008, voting systems submitted for certification shall stop the V-VPAT printer of all forward operations of the DRE if the printer is not working due to paper jams, out of supply of consumables, or other issue which may cause the correct readable printing of information on the V-VPAT record as designed.

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

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

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

(b) Voter's selections for the race information;

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

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

(e) Ability to optionally produce a unique serial number (randomized to protect privacy); and

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

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

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

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

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

45.5.2.9.24 The V-VPAT component shall be designed such that a voter shall not be able to leave the voting area with the paper record.

45.5.2.9.25 If used for provisional ballots, the V-VPAT system shall be able to mark paper records as a provisional ballot through the use of human readable text and optionally printing barcode and/or serial number information which shall provide for mapping the record back to both the electronic record and the provisional voter for processing after verification in accordance with Article 8.5 of Title 1 C.R.S.

45.5.2.9.26 The Secretary of State 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 Secretary of State 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) Printing ballots on demand;

(e) Hardware diagnostics testing;

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

(i) Absentee;

(ii) Early Voting;

(iii) Precinct/Poll Place;

(iv) Provisional; and

(v) Vote Center.

(g) Sealing and securing system devices;

(h) Logic and accuracy testing;

(i) Processing ballots;

(j) Accessible use;

(k) Accumulating results;

(l) Post-election audit;

(m) Canvass process handling;

(n) Audit steps and procedures throughout all processes;

(o) Certification of results; and

(p) Troubleshooting.

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

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

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

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

45.6.1.7 The voting system provider shall provide the same class of workstation and/or server for testing the voting system as the normal production environment for the State of Colorado.

45.6.2 Functional Testing

45.6.2.1 Voting system provider requirements for testing

45.6.2.1.1 The voting system provider shall submit for testing the specific system configuration that shall be offered to jurisdictions including the components with which the voting system provider recommends that the system be used.

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

45.6.2.1.3 The proprietary software shall be installed on the workstation/server and all applicable voting system components by the testing board following the verification of the trusted build, and using the procedures provided by the voting system provider. After installation, the software and firmware shall be verified to the trusted build hash values.

45.6.2.1.4 The test shall be performed with test ballots and an election setup file, as determined by the Secretary of State.

45.6.2.1.5 Functional testing shall be completed according to the schedule identified in section 45.3.3.

45.6.2.2 Secretary of State requirements for testing

45.6.2.2.1 The Secretary of State or the designee shall conduct functional testing on the voting system based on this rule and additional testing procedures as determined by the Secretary of State.

45.6.2.2.2 The voting system shall receive a pass/fail or not applicable for each test conducted with applicable notation on the test log.

45.6.2.2.3 A test log of the testing procedure shall be maintained and recorded on file with the Secretary of State. This test log shall identify the system and all components by voting system provider name, make,

model, serial number, software version, firmware version, date tested, test number, test description, notes of test, applicable test scripts, and results of test. All test environment conditions shall be noted.

45.6.2.2.4 All operating steps, the identity and quantity of simulated ballots, annotations of output reports, any applicable error messages 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; and

(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 at least three mock elections which shall include voting scenarios that exist within a primary, a coordinated election, and a recall 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. Test scripts shall be substantive and qualitative in form with expected results listed for each test.

45.6.2.3.5 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 as indicated in the instructions to providers.

45.6.2.3.6 The voting system provider is required to produce ballots in quantities identified below for each of the 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; and

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

45.6.2.3.7 All ballots provided shall be blank with no marks on them. The following combinations of ballots are required:

(a) Four separate decks of ballots shall be provided consisting of 25 ballots for each precinct/precinct split generated for each election that are flat (1500 minimum combined). At least one deck shall have the General Election data, and at least one shall have the Primary election data as indicated in the instructions for voting system providers;

(b) Four separate decks of ballots shall be provided consisting of 25 ballots for each precinct/precinct split generated for each election that are folded (1500 minimum combined). At least one deck shall have the General Election data, and at least one shall have the Primary election data as indicated in the instructions for voting system providers;

(c) Four separate decks of ballots consisting of 300 ballots of any single precinct from each election. Two of these decks shall be printed in all alternative languages as required for the State of Colorado pursuant to section 45.5.2.3.5;

(d) One separate deck of ballots consisting of 200 ballots of any single precinct from the Coordinated election shall be provided that contains a two page ballot (races on four faces);

(e) One separate deck of ballots consisting of 10 ballots for each precinct generated for the Recall election that are flat as indicated in the instructions for voting system providers; and

(f) Any voting system provider that uses serial numbers printed on ballots for processing shall produce ballots of each requirement above printed both with and without serial numbers.

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 Secretary of State or the designee.

45.6.2.3.9 The testing board shall mark a minimum of 300 ballots with marking devices of various color, weight, and consistency to determine accurate counting with a variety of marking devices.

45.6.2.3.10 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;

(d) Vote Center / DRE = 500

(e) Early Voting / OS = 5,000;

(f) Early Voting / DRE = 250;

(g) Absentee = 10,000; and

(h) Provisional = 5,000.

45.6.2.3.11 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 shall be designed and presented with a maximum of four (4) columns and a minimum of one (1) column.

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

45.6.2.3.13 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.

45.6.2.3.14 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 voter is allowed to vote in, regardless of party;

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

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

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

45.6.2.3.15 Additional tests and procedures may be requested at the discretion of the Secretary of State.

45.6.3 Certification

45.6.3.1 The Secretary of State shall certify voting systems that substantially comply with the requirements in this rule, Colorado Election Code, and any additional testing that is deemed necessary by the Secretary of State.

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

45.7 Temporary Use

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

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

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

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

45.8 Periodic Review

45.8.1 The Secretary of State shall periodically review the voting systems in use in Colorado to determine if the system(s):

(a) Are defective, obsolete, or unacceptable for use based on the requirements of this rule; and

(b) Have been modified from certified and trusted build versions of hardware or software;

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

45.8.3 The Secretary of State shall conduct an annual visual inspection of all software incident records maintained by each voting system provider certified for use in the State of Colorado.

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

45.8.5 All forms, notes and documentation from a periodic review shall be kept on file with the Secretary of State.

45.9 Decertification

45.9.1 If after any time the Secretary of State has certified a voting system, it is determined that the voting system fails to substantially meet the standards set forth in this rule, the Secretary of State shall notify any jurisdictions in the State of Colorado and the voting system provider of that particular voting system that the certification of that system for future use and sale in Colorado is to be withdrawn.

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

(a) The Election Assistance Commission (EAC);

(b) Voting Systems Testing Laboratories (VSTL);

(c) The Federal Election Commission (FEC);

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

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

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

(g) Information from any state elections department or Secretary of State; and/or

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

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

45.9.4 Pursuant to section 1-5-621, C.R.S., the Secretary of State shall hold a public hearing to consider the decision to decertify a voting system.

45.10 Modifications and Re-examination

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

45.10.2 A voting system provider may apply to the Secretary of State for the review of a modification of an existing certified system at any time during the year. Secretary of State shall conduct sufficient testing to ensure that all incremental changes to any voting system being submitted for certification meet all security requirements set forth in this rule.

45.11 Acceptance Testing by Jurisdictions

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

45.11.2 The voting system provider shall provide all manuals and training necessary for the proper operation of the system to the jurisdiction, or as indicated by their contract.

45.11.3 The election jurisdiction shall perform a series of functional and programming tests that shall test all functions of the voting system at their discretion.

45.11.4 The jurisdiction shall coordinate acceptance testing with the Secretary of State's designated agent and complete a Jurisdiction Acceptance Test form provided by the Secretary of State.

45.12 Purchases and Contracts

45.12.1 Any voting system that has been certified under the procedures of this Rule are eligible for purchase, lease, or rent for use by jurisdictions within the State of Colorado providing the contract contains the following items:

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

(b) Contract contains training and maintenance costs for Jurisdiction; and

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

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